Contributions à la Modélisation et à l'Évaluation de la Sûreté de Fonctionnement de Systèmes de Sécurité à Fonctionnalités Numériques

Florent Brissaud

Mémoire de thèse présenté en vue de l'obtention du titre de :

DOCTEUR DE L'UNIVERSITÉ DE TECHNOLOGIE DE TROYES

Spécialité : Optimisation et Sûreté des Systèmes

CONTRIBUTIONS À LA MODÉLISATION ET À L'ÉVALUATION DE LA SÛRETÉ DE FONCTIONNEMENT DE SYSTÈMES DE SÉCURITÉ À FONCTIONNALITÉS NUMÉRIQUES

Doctorant :
Florent Brissaud

Partenaires institutionnels :
Institut National de l'Environnement Industriel et des Risques (INERIS)
Université de Technologie de Troyes (UTT)

Mémoire de thèse révisé le :
3 janvier 2011

Thèse soutenue le 3 novembre 2010 devant le jury constitué de :

Prof. Mireille Bayart	Professeur des Universités	Président / Rapporteur
Prof. Yves Dutuit	Professeur des Universités Émérite	Rapporteur
Prof. Jean-Marc Thiriet	Professeur des Universités	Rapporteur
Prof. Marvin Rausand	Professor	Examinateur
Prof. Carol Smidts	Professor	Examinateur
M. Dominique Charpentier	Directeur Adjoint de la Certification, INERIS	Examinateur
Dr Anne Barros	Maître de Conférences	Directeur de Thèse
Prof. Christophe Bérenguer	Professeur des Universités	Directeur de Thèse
Dr Bruno Debray	Délégué Scientifique, INERIS	Membre Invité

À mon étoile…

Voilà que se répandit sur la montagne l'éclat froid qui précède le lever de la lune,
et que soudain la lune elle-même surgit derrière l'un des buissons frémissants.
Mais moi, je regardais entre-temps dans une autre direction et, quand je regardais de nouveau
devant moi et l'aperçus tout d'un coup, luisant déjà presque de toute sa rondeur, je m'immobilisai,
les yeux embués, car ma route pentue paraissait mener tout droit dans cette lune effrayante.
Mais au bout d'un petit moment je m'habituai à elle et observai méditativement comme son
ascension devenait pénible, jusqu'à ce qu'enfin, quand nous eûmes fait un bon bout de chemin à la
rencontre l'un de l'autre, je ressentisse une agréable somnolence qui, à mon sens,
m'envahissait à la suite des fatigues du jour, dont à vrai dire je ne me souvenais plus.

Franz Kafka,
Description d'un combat

REMERCIEMENTS

M'y voilà donc, face à cette page des remerciements. Cette page de début de mémoire mais dont la rédaction, paradoxalement, clôt ces années de thèse si bien remplies. Spontanément, mes premiers remerciements s'adressent à mes directeurs de thèse, Anne Barros et Christophe Bérenguer, qui m'ont suivi tout au long de ces trois années, encadré dans mon travail et épaulé face aux difficultés. Je sais à quel point avoir de bons directeurs de thèse est déterminant dans le déroulement d'un tel projet, ainsi que pour la suite que l'on souhaite y donner, et j'ai ainsi conscience de la chance importante dont j'ai bénéficié. Une nouvelle fois, un grand merci à tous les deux.

Je remercie sincèrement Dominique Charpentier, grâce à qui j'ai eu l'opportunité d'effectuer cette thèse au sein de l'INERIS, sur un sujet que nous avons eu l'occasion d'élaborer ensemble, et qui m'a confié l'autonomie me permettant de tirer pleinement avantage de ces années. Merci du travail fourni pour m'offrir ma chance dans la réalisation d'une thèse, et de la confiance qui m'a été donnée.

Très cordialement, je remercie Madame et Messieurs les Professeurs des Universités qui ont assuré la tâche de rapporteurs de ce mémoire, Mireille Bayart, Yves Dutuit et Jean-Marc Thiriet. Merci d'avoir consacré un temps important à la lecture attentive du mémoire, et d'avoir formulé des commentaires aussi judicieux et intéressants.

Je remercie chaleureusement Carol Smidts qui m'a permis d'être accueilli trois mois à l'Ohio State University, séjour dont j'ai beaucoup appris et qui offre à cette thèse une dernière partie très enrichissante. Merci pour ces nouveaux horizons, ainsi que de venir d'outre-Atlantique participer à mon jury de thèse.

Avec un certain enthousiasme, j'adresse un très grand merci à Marvin Rausand, tout d'abord pour m'avoir donné mes premiers cours de fiabilité et ainsi m'avoir transmis un fort intérêt pour cette discipline, puis, cinq ans plus tard, pour me faire l'honneur d'être membre de mon jury de thèse.

Merci à l'ensemble des membres du jury, rapporteurs, examinateurs, et directeurs de thèse, ainsi que Bruno Debray, pour avoir accepté l'invitation. C'est pour moi beaucoup de plaisir que de pouvoir soutenir ma thèse devant un tel jury.

Je remercie chacune des personnes avec qui j'ai eu la chance de travailler, collègues de l'INERIS, collègues et étudiants de l'UTT, d'autres entreprises et universités, toutes ces personnes qui m'ont permis de passer ces dernières années à réaliser une thèse dans de si bonnes conditions, avec beaucoup de plaisir et de passion. J'ai notamment une pensée particulière pour mes confrères de l'INERIS qui partagent la volonté de faire évoluer la maîtrise des risques industriels, et leur souhaite beaucoup de persévérances dans ces projets car, pour reprendre ces paroles d'un si grand homme, *ça sert à quoi l'cochonnet si t'as pas les boules*.

Avant de passer à des remerciements un peu plus personnels, je souhaiterais également vous remercier, vous qui prenez quelques instants pour lire ce mémoire. Dans ce mémoire, il y a le fruit de trois intenses années de travail, d'une passion pour un projet et pour une thématique. Dans ce mémoire, il y a un peu de moi. Celui-ci a avant tout été rédigé pour être lu, et j'espère donc que vous apprécierez parcourir ces pages, que vous y trouverez des éléments qui susciteront votre intérêt, et éventuellement qui vous amèneront même à réagir. Peut-être aurons-nous alors la possibilité d'en discuter.

Je vous souhaite une très bonne lecture.

Florent Brissaud

Je remercie du fond du cœur l'ensemble de mes proches, famille et amis, qui m'ont accompagné et soutenu tout au long de ces années, qui m'ont énormément donné, chacun à leur façon, et qui participent ainsi à la personne que je suis et aux projets que je réalise.

Merci de tout cœur.

à ma mère, pour être la première personne à m'encourager et à me soutenir inconditionnellement vers les projets les meilleurs pour son fils,

à mon père et à Magalie, pour constituer, avec ma mère, mon cercle familial auprès duquel je suis assuré de trouver le soutien essentiel en toute circonstance,

à Sarah, amie qui m'est si chère depuis l'adolescence, vers qui je sais me tourner dans les moments de doutes, et que j'ai tellement de plaisir à voir heureuse dans son tout jeune mariage,

à Michaël, avec qui les facéties ont toujours été une source inébranlable de créativité, et dont j'attends avec impatience les prochaines festivités où l'on se retrouvera, ainsi qu'avec Nicolas et Anne, autour d'un bon repas,

à Marie, dont la formidable force de conviction est devenue pour moi un modèle et une source de discernement face aux épreuves de la vie,

à Caro, avec qui les moments de complicité m'apportent tant de réjouissance, et les éclats de joie tant de réconfort,

à Flora, ma Flo, ma fée, dont le sourire me permet d'oublier le moindre souci, pour ne faire alors place qu'à un bonheur des plus tendres.

Florent.

SOMMAIRE

ACRONYMES

CTI	« Capteur-Transmetteur Intelligent » (utilisé pour qualifier un Capteur-Transmetteur à Fonctionnalités Numériques)	cf. Section I.3.1
EDD	Étude de Dangers	cf. Section I.1.1.2
EPR	Évaluation Probabiliste des Risques	cf. Section I.2.1.1
EUC	Équipement Commandé (ou Sous Contrôle)	cf. Section I.2.2.1
INERIS	Institut National de l'Environnement Industriel et des Risques	cf. Section I.1.2
PFD	Probabilité de Défaillance (dangereuse) à la Sollicitation (terme générique utilisé pour exprimer diverses indisponibilités)	cf. Section II.1.1
PPRT	Plan de Prévention des Risques Technologiques	cf. Section I.1.1.2
SCC	Système de Contrôle-Commande	cf. Section IV.1.1
SCR	Système de Contrôle en Réseaux	cf. Section IV.1.1
SID	Système à « Intelligence Distribuée »	cf. Section IV.1.1
SIS	Système Instrumenté de Sécurité	cf. Section I.2.2
UTT	Université de Technologie de Troyes	cf. Section I.1.3

NOTATIONS

A	évènement A
A = {…}	expression de l'évènement A
A_a	évènement de la ligne *a* du vecteur d'évènements A
$AB_{a,b}$	évènement de la ligne *a* et de la colonne *b* de la matrice d'évènements AB
A*	complément de l'évènement A (évènement « non » A)
$A \cup B$	union de l'évènement A et de l'évènement B (évènement A « ou » B)
$\bigcup_a A_a$	union des évènements A_a suivant les valeurs possibles de la variable *a* (avec des conditions éventuelles sur la variable *a*)
$A \cap B$	intersection de l'évènement A et de l'évènement B (évènement A « et » B)
$\bigcap_a A_a$	intersection des évènements A_a suivant les valeurs possibles de la variable *a* (avec des conditions éventuelles sur la variable *a*)
*P[*A*]*	probabilité de l'évènement A
*P[*A | B*]*	probabilité de l'évènement A sachant l'évènement B
*P[*A*](t)*	probabilité de l'évènement A en fonction de la variable *t*
X	variable aléatoire *X*
E[X]	espérance de la variable aléatoire *X*
$E^2[X]$	espérance à la puissance *2* de la variable aléatoire *X*
V[X]	variance de la variable aléatoire *X*
$f_X(x)$	densité de probabilité de la variable aléatoire *X*
x	variable *x*
x(t)	variable *x* en fonction de la variable *t*
x(t, i)	variable *x* en fonction des variables *t* et *i*
$x \in D$	la variable *x* appartient au domaine *D* (qui peut être un ensemble ou un intervalle)
$x \in \mathbb{R}$	la variable *x* est un nombre réel
$x \in \mathbb{N}$	la variable *x* est un nombre entier
$\boldsymbol{x}$	variable $\boldsymbol{x}$ de type vecteur
$\boldsymbol{x} \in \mathbb{R}^N$	la variable $\boldsymbol{x}$ de type vecteur est composée de *N* nombres réels
$\boldsymbol{x} \in \mathbb{N}^N$	la variable $\boldsymbol{x}$ de type vecteur est composée de *N* nombres entiers
(x, y)	ensemble constitué des variables *x* et *y*
[x ; y[	intervalle allant de la valeur *x* (incluse) à la valeur *y* (non incluse)
$\boldsymbol{x}_a$	composante de la ligne *a* de la variable $\boldsymbol{x}$ de type vecteur
$M_{a,b}$	composante de la ligne *a* et de la colonne *b* de la variable *M* de type matrice
$\sum_{i=a}^{b} x(i)$	somme des variables *x(i)* suivant la variable *i* allant de *a* à *b*
$\sum_i x(i)$	somme des variables *x(i)* suivant les valeurs possibles de la variable *i* (avec des conditions éventuelles sur la variable *i*)
$\prod_{i=a}^{b} x(i)$	produit des variables *x(i)* suivant la variable *i* allant de *a* à *b*
$\prod_i x(i)$	produit des variables *x(i)* suivant les valeurs possibles de la variable *i* (avec des conditions éventuelles sur la variable *i*)

$max(x)$	maximum des valeurs possibles de la variable x
$max(x, y)$	maximum parmi les valeurs x et y
$arg\ max(x(t))$	valeur de la variable t qui maximise la fonction $x(t)$
$min(x)$	minimum des valeurs possibles de la variable x
$min(x, y)$	minimum parmi les valeurs x et y
$arg\ min(x(t))$	valeur de la variable t qui minimise la fonction $x(t)$
e^x	fonction exponentielle de x ($e^x = exp(x)$)
$exp(x)$	fonction exponentielle de x ($exp(x) = e^x$)
$abs(x)$	valeur absolue de x
$\|\|\boldsymbol{x}\|\|$	norme euclidienne du vecteur $\boldsymbol{x}$
$\boldsymbol{x}^T$	transposée du vecteur $\boldsymbol{x}$
$\frac{d}{dt}x(t)$	dérivée de la fonction $x(t)$ suivant la variable t
$\int_u^v x(t) \cdot dt$	intégration de la fonction $x(t)$ suivant la variable t allant de u à v
$\binom{n}{k}$	fonction combinatoire de k parmi n
$k!$	fonction factorielle de k

D'autres notations sont spécifiques à la Section IV.3 et sont données dans le Tableau IV.3.1.

PRÉFACE

La thèse de doctorat présentée dans ce mémoire a été réalisée à l'Institut National de l'Environnement Industriel et des Risques (INERIS), et sous la direction scientifique de l'Université de Technologie de Troyes (UTT). Le contexte général est celui de la maîtrise des risques technologiques, et plus particulièrement celui de l'évaluation probabiliste des risques. Le sujet concerne quant à lui la sûreté de fonctionnement de systèmes relatifs à la sécurité, notamment ceux intégrant des fonctionnalités numériques, et plus spécifiquement les capteurs-transmetteurs communément qualifiés d' « intelligents ».

En France, la réglementation sur la maîtrise des risques technologiques intègre des évaluations probabilistes depuis la « loi Risques » de 2003, par l'intermédiaire des études de dangers (EDD) et des plans de prévention des risques technologiques (PPRT). La généralisation de ces considérations à l'ensemble des activités industrielles étant relativement récente, certains aspects essentiels à la pertinence des évaluations – interprétation des probabilités, concepts d'incertitudes – mériteraient encore d'être mieux assimilés. De même, les évaluations de sûreté de fonctionnement sont relativement sommaires dans les EDD et les PPRT actuellement réalisés. À cela s'ajoute les problématiques induites par l'utilisation de nouvelles technologies au sein de systèmes relatifs à la sécurité, qui posent certaines difficultés particulières à ce type d'évaluations. Ce contexte introductif de la thèse est présenté dans le Chapitre I de ce mémoire. Aujourd'hui, la nécessité est ainsi de disposer d'outils et de méthodes d'évaluation relativement simples à mettre en place, et qui permettraient de répondre au mieux à la complexité des systèmes, afin d'améliorer la pertinence et l'efficacité de la prise de décision dans la maîtrise des risques technologiques.

Face à l'ensemble de ces problématiques, nous avons choisi de mener ces travaux de thèse sur plusieurs fronts. L'objectif était ainsi de répondre à un spectre assez large de préoccupations exprimées par l'INERIS et ses principaux partenaires (Ministère de l'Enseignement Supérieur et de la Recherche, Ministère de l'Écologie et du Développement Durable) en termes de modélisation et d'évaluation de la sûreté de fonctionnement de systèmes relatifs à la sécurité, et des problématiques associées liées aux nouvelles technologies. Du plus général au plus spécifique, la sûreté de fonctionnement des systèmes suivants a alors été considérée : systèmes relatifs à la sécurité en général ; capteurs-transmetteurs à fonctionnalités numériques, communément qualifiés de « capteurs-transmetteurs intelligents » (CTI) ; et systèmes de contrôle-commande (SCC) intégrant des CTI. Les travaux de thèse ont alors dû traiter des enjeux particuliers à chacun de ces trois niveaux d'étude, et les outils et méthodes apportés en réponse aux problématiques correspondantes sont respectivement présentés dans les Chapitres II, III, et IV.

Le Chapitre II a pour objectif d'apporter certaines contributions à l'évaluation de la sûreté de fonctionnement de systèmes relatifs à la sécurité en général. Pour cela, des expressions générales sont proposées afin d'évaluer des probabilités de défaillance de systèmes d'architectures redondantes, et soumis à des tests de révision partiels et complets. Une méthodologie est également introduite pour l'évaluation des taux de défaillance (paramètres d'entrée des expressions précédentes) en fonction des facteurs d'influence propres aux systèmes considérés (incluant notamment des conditions environnementales et opérationnelles). L'intérêt de ce type d'approches probabilistes pour la maîtrise des risques technologiques est illustré par des cas d'étude.

L'évaluation, plus spécifique, de la sûreté de fonctionnement des « capteurs-transmetteurs intelligents » (CTI) est le sujet du Chapitre III. Afin de prendre en compte les particularités des CTI, notamment les interactions internes (matérielles et fonctionnelles) ainsi que les comportements mal connus en cas de défauts ou de défaillances, une modélisation adaptée est proposée. Des analyses de fiabilité basées sur ce modèle sont ensuite développées, permettant d'évaluer les effets des défauts et défaillances sur les éléments matériels et les fonctions du système, ainsi que les probabilités de dysfonctionnements et de modes de défaillance. Enfin, des analyses d'incertitudes testent la robustesse de ces évaluations face aux incertitudes liées aux paramètres et au modèle. La mise en œuvre de ces approches est illustrée par un cas d'étude.

Dans le Chapitre IV, les CTI sont ensuite considérés en tant qu'éléments de systèmes de contrôle-commande (SCC). Les évaluations de sûreté de fonctionnement de tels systèmes doivent alors prendre en compte les interactions entre les éléments du système, et en particulier entre les CTI, ainsi que les interactions avec le processus contrôlé. Une approche formalisée de fiabilité dynamique est développée afin de répondre à ces problématiques tout en intégrant les particularités des CTI (notamment les capacités d'échanger et de traiter des informations). Un cas d'étude relativement complet permet d'illustrer les possibilités de modélisation et d'évaluation offertes par l'approche proposée.

Le Chapitre V présente des conclusions et des perspectives de ces travaux de thèse ; le Chapitre VI regroupe les annexes ; et le Chapitre VII référence les citations faites tout au long de ce mémoire, ainsi que les publications réalisées lors de ces travaux de thèse.

CHAPITRE I

CONTEXTE INTRODUCTIF

Ce chapitre présente le contexte général dans lequel s'est déroulé la thèse, qui est celui de la maîtrise des risques technologiques, et plus particulièrement de l'évaluation probabiliste de ces risques ; et le sujet central de la thèse, qui est la sûreté de fonctionnement des systèmes relatifs à la sécurité, et plus spécifiquement celle des « capteurs-transmetteurs intelligents » (CTI).

La première section de ce chapitre est une présentation du contexte industriel de la thèse, effectuée à l'Institut National de l'Environnement Industriel et des Risques (INERIS), et sous la direction scientifique de l'Université de Technologie de Troyes (UTT). La seconde section approfondit certains concepts de l'évaluation probabiliste des risques et des systèmes instrumentés de sécurité. La troisième section introduit les CTI ainsi que les problématiques liées à l'évaluation de la sûreté de fonctionnement de ces systèmes. Enfin, la quatrième section propose une grille de lecture de ce mémoire de thèse.

SOMMAIRE DU CHAPITRE I

I.1. CONTEXTE INDUSTRIEL

I.1.1. La Maîtrise des Risques Technologiques en France

I.1.1.1. Prélude

Depuis les Révolutions Industrielles des XVIIIème et XIXème siècles, le développement de nouvelles technologies n'a cessé de croître, souvent à des allures exponentielles (cf. Lois de Moore [DHu05]). Aujourd'hui, le contexte est celui de la globalisation. Les systèmes doivent alors répondre à de constantes évolutions et à des performances accrues, tout en faisant face à de très fortes contraintes économiques, humaines, et à des ressources limitées. Cela a conduit au développement de technologies de plus en plus critiques pour la sécurité. Les exemples se trouvent dans de nombreux secteurs d'activités : l'énergie (les puissances des centrales électriques, le nucléaire, les exploitations offshores), le transport (la capacité des avions, la vitesse des trains), et l'industrie en général (l'utilisation de nouveaux procédés, de nouvelles substances). La maîtrise des risques liés aux activités technologiques est alors devenue une nécessité sociétale, environnementale, et économique. Pour répondre aux exigences de l'ensemble de ces domaines, l'évaluation des risques doit faire face à plusieurs défis, dont celui de prendre en compte de manière efficace et réaliste toute la complexité grandissante des systèmes.

I.1.1.2. Cadre réglementaire français sur les risques technologiques

En France, la réglementation sur les risques technologiques repose sur la réglementation des *installations classées pour la protection de l'environnement* (ICPE), instaurée dans les années soixante-dix [JO76], et régie par le Code de l'Environnement [CdE09]. À l'origine, ce cadre réglementaire est exclusivement « déterministe », c'est-à-dire qu'il ne prend en compte que certains scénarios d'accidents de référence qui sont jugés comme les plus graves. Cependant, cette vision du risque s'est montrée trop restrictive. En effet, un risque est caractérisé par un scenario (ou un évènement), une gravité (conséquences non désirées), ainsi que par une probabilité (ou parfois une « fréquence ») [SKa91]. L'approche naturelle et la plus complète d'une évaluation d'un risque est donc une approche probabiliste. Dans l'industrie du nucléaire, ce type d'approche est apparu dès les années soixante-dix, aux États-Unis d'Amérique, mais également en France [ALa08]. En revanche, pour l'industrie française en général, la réglementation sur les risques technologiques n'a intégré des critères probabilistes qu'à la suite de la catastrophe d'AZF à Toulouse, en septembre 2001.

C'est la « loi Risques » du 30 juillet 2003 [JO03] relative à la prévention des risques technologiques, et précisée par le décret du 7 septembre 2005 [JO05b], qui a introduit pour la première fois la notion « d'aléa technologique » dans la réglementation française [MED07]. (La « loi Risques » a également été suivie par de nombreuses circulaires d'application qui ont ensuite été récapitulées dans la circulaire du 10 mai 2010 [Cir10].) Un « aléa » est défini par la circulaire du 7 octobre 2005 [Cir05] comme la « probabilité qu'un phénomène accidentel produise en un point donné des effets d'une intensité donnée, au cours d'une période donnée » (à noter que l' « intensité des effets » fait référence à la « gravité des conséquences potentielles », et doit ainsi être distinguée de la « gravité » qui inclut, en plus, la « vulnérabilité des cibles aux effets »). Cette notion d' « aléa technologique » prend son sens dans le contexte des *plans de prévention des risques technologiques* (PPRT) introduits par la « loi Risques » [JO03]. Les PPRT visent à mieux encadrer l'urbanisation aux abords des ICPE (et à résoudre les situations difficiles en matière d'urbanisme héritées du

passé), en prévoyant, pour une zone d'aléa donnée, des actions sur [MED07] : l'urbanisme (limitations de constructions) ; les usages (restrictions sur les espaces publics) ; le bâti (renforcements de protections, par exemple par des vitrages appropriés) ; et le foncier (préemptions, délaissements, expropriations).

Rappelons que les ICPE comprennent : le régime de déclaration (D), (dont celui de déclaration avec contrôle (DC)), pour les activités relativement moins polluantes et dangereuses, et qui concernent environ 450 000 installations en France, dont 7 000 nouvelles en 2009 [MEE10a] ; le régime d'autorisation (A), (dont celui simplifié d'enregistrement (E)), pour les activités qui présentent les risques les plus importants, qui concernent environ 46 000 installations en France, dont 1 750 nouvelles en 2009 [MEE10a]. De plus, selon la directive européenne dite « Seveso » [CE96] (qui fait suite à la catastrophe de Seveso en Italie, en juillet 1976), une installation soumise à autorisation peut aussi être classée « Seveso seuil bas » (524 en France, en 2009 [MEE10a]) ou « Seveso seuil haut » (616 en France, en 2009 [MEE10a]). Les installations classées « Seveso seuil haut » sont alors soumises à un régime d'autorisation particulier dit « avec servitudes d'utilité publique » (AS), et sont les seules concernées par les PPRT. Au début de l'année 2010, ce sont 420 PPRT qui ont été réalisés, dont 30 ont été approuvés, l'objectif étant d'atteindre 80% de PPRT approuvés d'ici fin 2011 [MEE10b].

La « loi Risques » [JO03] a également fait évoluer la réglementation sur les *études de dangers* (EDD) afin, notamment, d'y intégrer des critères probabilistes. Les EDD concernent toutes les ICPE soumises à autorisation (A et AS) et sont, en particulier, un préalable aux PPRT. (D'ailleurs, parmi les plus grandes difficultés méthodologiques observées lors de l'élaboration des PPRT s'est trouvé la façon dont les risques devaient être évalués et pris en compte dans le cadre des EDD [GRa09].) Une EDD a pour objet de « rendre compte de l'examen effectué par l'exploitant pour caractériser, analyser, évaluer, prévenir et réduire les risques d'une installation ou d'un groupe d'installations » [Cir06]. Le Code de l'Environnement [CdE09], ainsi modifié par la « loi Risques », précise que :

- « cette étude donne lieu à une analyse de risques qui prend en compte la probabilité d'occurrence, la cinétique et la gravité des accidents potentiels selon une méthodologie qu'elle explicite » ;
- « elle définit et justifie les mesures propres à réduire la probabilité et les effets de ces accidents. »

À noter que « la probabilité d'occurrence d'un accident est assimilée à sa fréquence d'occurrence future estimée sur l'installation considérée » [Cir05]. Des précisions sur les méthodes d'évaluation sont apportées par l'arrêté du 29 septembre 2005 [JO05a], et la circulaire du 7 octobre 2005 [Cir05] : « Pour l'évaluation de la probabilité d'occurrence d'un phénomène dangereux (…), la méthode est libre (…). Cependant, une attention particulière doit être portée à la pertinence de la méthode utilisée, qui doit être intimement liée à l'analyse de risques et confrontée au retour d'expérience » [Cir05] ; « Cette méthode utilise des éléments qualifiés ou quantifiés tenant compte de la spécificité de l'installation considérée. Elle peut s'appuyer sur la fréquence des évènements initiateurs spécifiques ou génériques et sur les niveaux de confiance des mesures de maîtrise des risques agissant en prévention ou en limitation des effets » [JO05a]. Dans la suite, l'attention sera portée sur ces « mesures de maîtrise des risques ».

Trois critères de performance d'une « mesure de maîtrise des risques » (ou « barrière de sécurité ») sont retenus par la circulaire du 7 octobre 2005 [Cir05] : l'efficacité, qui est la « capacité à remplir la mission/fonction de sécurité qui lui est confiée pendant une durée donnée et dans son contexte d'utilisation » ; le temps de réponse, qui est « l'intervalle de temps entre la sollicitation et l'exécution de la mission/fonction de sécurité » ; et le niveau de confiance, qui est « l'architecture

(redondance éventuelle) et la classe de probabilité, inspirés des normes NF EN 61508 et CEI 61511, pour qu'une barrière, dans son environnement d'utilisation, assure la fonction de sécurité pour laquelle elle a été choisie. Cette classe de probabilité est déterminée pour une efficacité et un temps de réponse donnés. Ce niveau peut être déterminé suivant les normes NF EN 61508 et CEI 61511 pour les systèmes instrumentés de sécurité » (cf. Section I.2.2 pour plus de détail sur la norme NF EN 61508, également nommée CEI 61508, ainsi que sur la norme CEI 61511). C'est ainsi par l'intermédiaire du « niveau de confiance » d'une « mesure de maîtrise des risques » que la réglementation française demande des évaluations probabilistes. Dans sa mise en pratique, l'un des principaux problèmes rencontrés pour prendre en compte ces probabilités est alors lié aux calculs de fiabilité des barrières de sécurité [GRa09] (cf. Section I.3.2.2 pour la définition de la fiabilité).

Pour conclure sur ce cadre réglementaire, la « loi Risques » apporte une évolution importante à la maîtrise des risques technologiques en France, grâce à l'intégration de critères probabilistes. Cette probabilité permet en effet de définir convenablement un risque, comme il en était déjà question notamment dans l'industrie nucléaire. En matière d'urbanisme, il est alors possible d'ajuster au mieux l'affection et l'utilisation des sols autour des installations [GRa09]. On peut cependant regretter quelques faiblesses dans l'utilisation de certaines notions, notamment de par l'arrêté du 29 septembre 2005 [JO05a] et la circulaire du 7 octobre 2005 [Cir05] (reprise par la circulaire du 10 mai 2010 [Circ10]). En particulier, certains termes sont probablement mal définis, et ainsi sources de confusion. Par exemple, une « probabilité » (nombre réel entre *0* et *1*, sans unité) ne doit pas être confondue avec une « fréquence » (nombre réel supérieur à *0*, éventuellement plus grand que *1*, et en unité inverse du temps) ; de plus, la définition d' « efficacité » semble incluse dans celle de « niveau de confiance » (avec quelques nuances peu différentiables telles que « contexte d'utilisation » et « environnement d'utilisation », ainsi que « fonction de sécurité qui lui est confiée » et « fonction de sécurité pour laquelle elle a été choisie ») ; enfin, « efficacité » et « temps de réponse » sont deux critères qui devraient faire partie intégrante d'une définition appropriée d'une « fonction de sécurité ». En outre, plusieurs termes semblent avoir été créés par ces textes réglementaires, alors que nombre d'entre eux sont étroitement liés à des notions bien connues et utilisées dans les milieux scientifiques. Par exemple, les « études de dangers » ou « analyses de risques » semblent idéalement se rapporter à des « évaluations probabilistes des risques » ; les « performances » des « mesures de maîtrise des risques » sont liées à la « sûreté de fonctionnement » ; les « niveaux de confiance » sont définis par des « indisponibilités » ; et l' « efficacité » fait référence à des « défaillances systématiques ». Ces notions issues de la littérature scientifique sont développées tout au long de ce présent chapitre. Dans la suite de ce mémoire de thèse, ces termes seront préférés à ceux introduits par la réglementation française.

I.1.2. Le Rôle de l'INERIS dans la Maîtrise des Risques Technologiques

L'Institut National de l'Environnement Industriel et des Risques (INERIS) est un établissement public à caractère industriel et commercial (EPIC), placé sous la tutelle du Ministère de l'Écologie, de l'Énergie, du Développement Durable et de la Mer (MEEDDM), (appellation en cours au début de l'année 2010). La mission affichée de l'INERIS est de réaliser des études et des recherches permettant de prévenir les risques que les activités économiques font peser sur la santé, la sécurité des personnes, les biens, et l'environnement, et de fournir toute prestation destinée à faciliter l'adaptation des entreprises à cet objectif [INE10]. L'INERIS effectue ainsi à la fois une mission de service public, pour l'État et les collectivités (programmes de recherche, appuis techniques, formations), et des prestations commerciales, d'étude et de conseil, pour des clients privés.

En ce qui concerne la maîtrise des risques technologiques, l'INERIS intervient à deux niveaux : celui des installations industrielles, notamment par la réalisation d'EDD et l'accompagnement pour les procédures de PPRT (cf. Section I.1.1.2) ; et celui des équipements, en particulier par l'évaluation de dispositifs de sécurité. Sur ce dernier point, l'INERIS est dotée d'une direction de la certification qui est notamment accréditée pour certifier des systèmes selon les normes en sécurité fonctionnelle CEI 61508 et CEI 61511 (cf. Section I.2.2). Afin de répondre à ses missions, l'INERIS a ainsi besoin de mener des travaux de recherche pour développer des outils méthodologiques et des référentiels, pour l'évaluation probabiliste des risques et de la sûreté de fonctionnement.

I.1.3. Thèse de Doctorat INERIS-UTT, en contrat CIFRE

La thèse de doctorat présentée dans ce mémoire a été réalisée à l'INERIS, à Verneuil-en-Halatte dans l'Oise, sous la direction scientifique de l'Université de Technologie de Troyes (UTT), à Troyes dans l'Aube, dans le cadre d'une convention industrielle de formation par la recherche (CIFRE), initiée en octobre 2007.

En tant que CIFRE, cette thèse a été en grande partie financée par le Ministère de l'Enseignement Supérieur et de la Recherche (MESR), par l'intermédiaire de l'Association Nationale de la Recherche et de la Technologie (ANRT). Au sein de l'INERIS, le principal financement a été apporté par un programme de recherche (dit « programme 190 » [INE09]), également financé par le Ministère de l'Enseignement Supérieur et de la Recherche, et intitulé « Qualification de la sûreté de fonctionnement des systèmes industriels » (QUASSI). Certains travaux (ceux présentés dans le Chapitre II de ce mémoire), ont également été réalisés dans le cadre d'un programme d'appui technique (dit « programme 181 ») au Ministère de l'Écologie, sur l'évaluation des performances des barrières techniques de sécurité.

À l'origine, l'unité d'accueil de l'INERIS était le Laboratoire d'Évaluation des Équipements Électriques (LEEL), au sein de la Direction de la Certification (DCE). Suite à une réorganisation de l'INERIS au cours de l'année 2008, un transfert a eu lieu vers l'unité Barrières Techniques et Systèmes de Sécurité (BT2S), du pôle Évaluation des Équipements et des Systèmes de Sécurité (2E2S), au sein de la Direction des Risques Accidentels (DRA).

Le laboratoire d'accueil de l'UTT a quant à lui été le Laboratoire de Modélisation et Sûreté des Systèmes (LM2S), rattaché au pôle Recherche Opérationnelle, Statistique Appliquées et Simulation (ROSAS), au sein de l'Institut Charles Delaunay (ICD) dont le cadre thématique se définit autour des « Sciences et Technologies pour la Maîtrise des Risques » (STMR). L'ICD est associé au Centre National de la Recherche Scientifique (CNRS) sous forme d'une Formation de Recherche en Évolution (FRE, numéro 2848) depuis 2006, puis sous forme d'une Unité Mixte de Recherche (UMR, numéro 6279) portant le nom de STMR, au cours de l'année 2010.

Les travaux de thèse ont été réalisés en majeur partie à l'INERIS, avec des visites fréquentes à l'UTT. De plus, trois mois (de février à avril 2010) se sont déroulés à l'Université d'État de l'Ohio (OSU), à Columbus, aux États-Unis d'Amériques, dans le cadre d'une collaboration scientifique. Les résultats de ces derniers travaux sont présentés dans la Section IV.3 de ce mémoire de thèse.

I.2. ÉVALUATION PROBABILISTE DES RISQUES

I.2.1. Concepts Fondamentaux pour l'Évaluation Probabiliste des Risques

I.2.1.1. Introduction à l'évaluation probabiliste des risques

L'*évaluation probabiliste des risques* (EPR), (ou « *évaluation probabiliste de sécurité* » (EPS), « *analyse quantitative des risques* » (AQR) ; et en anglais, « *probabilistic risk assessment* » (PRA), « *probabilistic safety assessment* » (PSA), et « *quantitative risk analysis* » (QRA)), est devenue un outil de maîtrise des risques largement utilisé et accepté dans de nombreux secteurs d'activité, notamment le nucléaire (qui utilise alors le terme de « sûreté » au lieu de « sécurité »), l'aérospatial, la pétrochimie, et l'industrie des procédés en général. Le principal sujet d'une EPR consiste à identifier les scénarios possibles d'accident (séquences d'évènements qui pourraient conduire à un accident, ou à tout autre évènement non souhaité), à évaluer leurs conséquences (gravités), et à quantifier leurs probabilités (ou parfois leurs « fréquences »). Pour cela, l'approche la plus commune est basée sur les arbres d'évènement et de défaillance, initiée dans les années soixante-dix par les études de sécurité des réacteurs nucléaires [USN75, ALa08].

Les arbres d'évènement sont des techniques inductives qui développent les évènements possibles (jusqu'aux évènements finaux, qui peuvent être des accidents ou non) faisant suite à un évènement initiateur, prenant en compte les réalisations et non-réalisations des fonctions de sécurité (suite aux états fonctionnels des systèmes relatifs à la sécurité, dont notamment des barrières de sécurité, cf. Section I.2.2), tel que décrit sur la Figure I.2.1. En complément, les arbres de défaillance sont des techniques déductives qui illustrent et expriment les fonctions de sécurité (dont les non-réalisations sont représentées en tant qu'évènements sommet) par des combinaisons d'évènements basiques (réalisations ou non-réalisations de sous-fonctions), en utilisant des portes logiques (notamment de type « et » et « ou »), tel que décrit sur la Figure I.2.2. Les analyses sont ensuite classiquement effectuées sur la base d'un formalisme mathématique exploitant de l'algèbre booléenne. Pour l'application de ces méthodes, de nombreuses références spécifiques peuvent être trouvées dans la littérature, et notamment le guide relativement complet et en libre accès de l'administration américaine de l'aéronautique et de l'espace (NASA) [MSt02]. Dans ce Chapitre I, ces outils ne sont pas présentés d'un point de vue « technique ». Nous avons cependant souhaité développer certains concepts fondamentaux que sont les notions de probabilités et les concepts d'incertitudes, respectivement présentées dans les Sections I.2.1.2 et I.2.1.3. Ces discussions permettent notamment d'exposer une certaine « philosophie générale » des évaluations probabilistes des risques, qui a été adoptée lors de ces travaux de thèse.

I.2.1.2. Notions de probabilités dans le contexte des EPR

Parce que les EPR doivent traiter avec des évènements qui sont généralement (et heureusement) rares, et même parfois jamais observés, les probabilités manipulées sont plus justement interprétées comme étant subjectives plutôt que des fréquences relatives (malgré les définitions données dans la réglementation française sur les risques technologiques, cf. Section I.1.1.2). En particulier, le manque de données appropriées et le recours (indispensable) à des « jugements » implique cette subjectivité [GAp88, GAp90, RWi96]. En effet, l'interprétation fréquentiste (ou « physique ») des

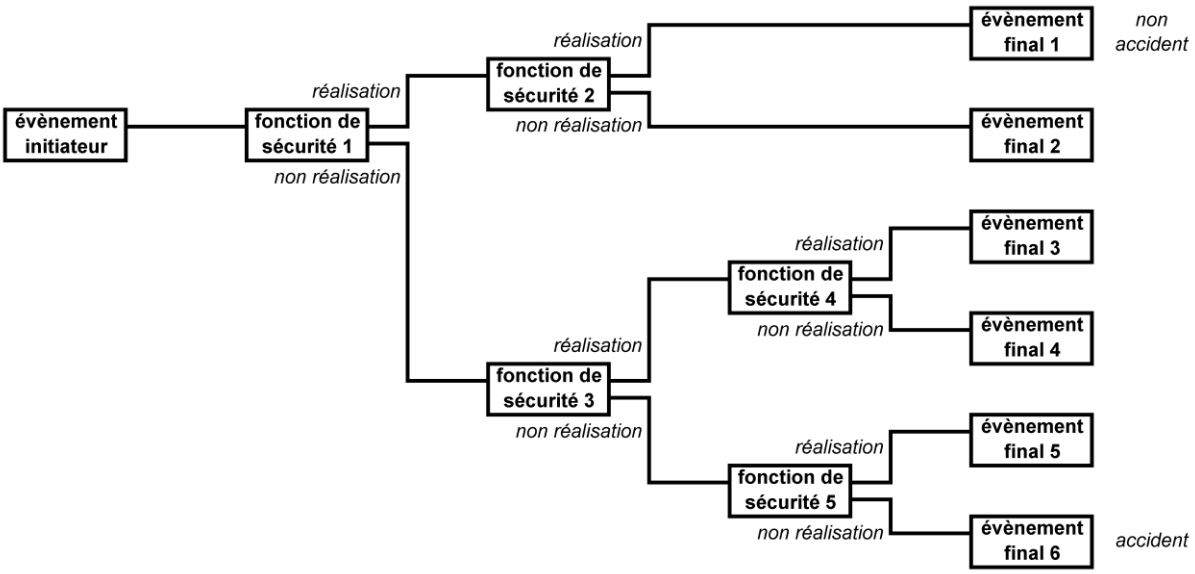

Figure I.2.1. Exemple conceptuel d'un arbre d'évènement

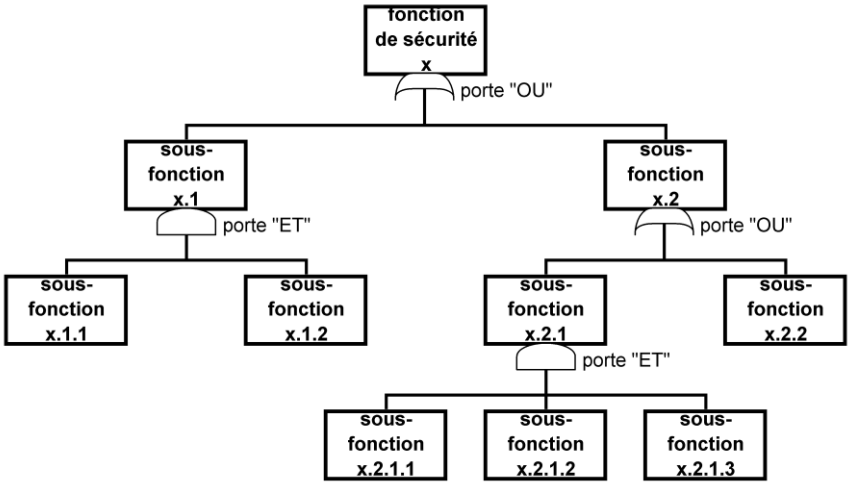

Figure I.2.2. Exemple conceptuel d'un arbre de défaillance

probabilités n'a de sens que lorsque sont considérés des « tirages » (ou « essais », « expériences ») identiques. La probabilité d'un évènement est alors définie par sa fréquence relative d'occurrence au cours d'une longue série (qui tend vers l'infini) de ces « tirages » (cette « fréquence relative » est ainsi sans dimension et peut effectivement définir une probabilité, contrairement à une simple « fréquence » qui est de dimension inverse du temps). Cependant, les occurrences d'évènements tels que des défaillances de systèmes ou des erreurs humaines sont souvent le fait de caractéristiques ou de conditions environnementales qui leurs sont propres, rendant le concept de « tirages identiques » inapproprié. En revanche, dans l'interprétation subjective (ou « bayésienne »), une probabilité mesure un « degré de croyance » (ou « l'état des connaissances »), fournissant ainsi un indicateur qui est manipulé suivant les règles mathématiques des probabilités.

Un premier argument en faveur des probabilités subjectives est que la plupart des évènements (tous ?) se produisant dans le monde se conforment à des lois physiques ou chimiques (et déterministes, ou du moins, si on laisse ici de coté la mécanique quantique). Par exemple, même le résultat d'un lancer de dé pourrait théoriquement être déterminé si l'on connaissait la position initiale du dé, son poids, la force et la direction du lancer, les propriétés des surfaces en contact, etc. Toutefois, ces lois et paramètres décisifs n'étant pas suffisamment connus pour permettre de prédire de tels évènements, des probabilités sont utilisées. Un second argument peut, par exemple, être illustré par l'évènement suivant : « un accident se produira avant la fin de cette année ». Quelle que soit la probabilité attribuée a priori à cet évènement, une fois l'année écoulée, il sera possible d'y répondre par « oui » ou par « non », c'est-à-dire que la probabilité qui est vérifiée comme « vraie » ne peut être que *0* (pour la non-occurrence) ou *1* (pour l'occurrence). De plus, la probabilité attribuée à cet évènement pourrait être ajustée au fur et à mesure que l'année s'écoule (par exemple, en utilisant des inférences bayésiennes), rendant cet évènement de moins en moins probable s'il ne s'est toujours pas produit, et à défaut de nouvelles informations. Pour résumer, une probabilité est finalement un degré de croyance en un évènement, résultant d'une certaine quantité d'information (incluant, par exemple, de potentielles données issues du retour d'expérience), et à un instant donné. En particulier, différentes personnes peuvent obtenir différentes probabilités pour un même évènement [RWi96] (ce qui, en pratique, est le cas).

Bien qu'une probabilité ne puisse, par nature, pas être « vraie » d'après l'interprétation subjective (à moins de ne prendre comme valeur *0* ou *1*), des critères pertinents peuvent cependant être définis : la cohérence, la consistance, et la robustesse. La cohérence signifie que si l'état des connaissances situe un évènement ou un scénario globalement plus vraisemblable qu'un autre, alors les probabilités qui leurs sont attribuées doivent refléter cet ordre. Afin de remplir cette caractéristique, des méthodes et des modèles harmonisés (par exemple, des arbres d'évènement et de défaillance) doivent être utilisées pour exprimer des probabilités qui dépendent logiquement des informations d'entrée (paramètres). Lorsque ces approches prennent en compte un maximum d'information, les résultats peuvent être jugés comme étant consistants. Enfin, les incertitudes dans les informations d'entrée ne devraient avoir qu'un impact minimal sur la cohérence des résultats, ce qui signifie que les résultats ont de faibles incertitudes, et sont donc robustes. Les concepts d'incertitudes sont le sujet de la section suivante.

I.2.1.3. Concepts d'incertitudes dans le contexte des EPR

Il paraît difficile de donner une définition à l' « incertitude » qui ne soit pas un pléonasme, et qui soit plus perceptible que le mot en lui-même. Aussi, nous ne nous risquerons pas ici à cette tâche. Pour autant, l'identification des sources d'incertitudes est une partie importante des EPR [GAp90], et les analyses d'incertitudes sont devenues un champ d'intérêt notable, en particulier lorsqu'il est

question de systèmes complexes [JHe96]. Les analyses d'incertitudes sont définies comme la détermination des incertitudes dans les résultats (par exemple, des résultats d'analyses par arbre de défaillance), qui ont pour origine les incertitudes dans les données (informations) d'entrée [JHe06]. De telles analyses sont présentées dans un autre chapitre de ce mémoire de thèse (cf. Sections III.2.2.3 et III.3.3). L'objectif de cette section est de présenter les différents concepts d'incertitudes dans le contexte des EPR.

Des distinctions entre « types d'incertitudes » ont été faites dans de nombreux travaux portant sur des EPR (et sur la sûreté de fonctionnement en général). La différence la plus commune est celle entre les « incertitudes aléatoires » (ou « de type A », « stochastiques », « irréductibles »), qui proviennent des caractères aléatoires inhérents aux comportements des systèmes, et les « incertitudes épistémiques » (ou « de type B », « subjectives », « réductibles »), qui proviennent des manques de connaissance sur les valeurs à attribuer à certaines quantités fixées [JHe96, WOb04, JHe06]. Cette différence est cependant souvent remise en cause [RWi96], en particulier au regard de l'interprétation subjective des probabilités qui implique que le caractère « aléatoire » n'existe pas vraiment (« Dieu ne joue pas aux dés »), et que l'incertitude provient donc toujours d'un manque de connaissance, c'est-à-dire « épistémique ». Néanmoins, cette distinction peut aussi être simplement adoptée pour des raisons de convenance [GAp90, EZi96], pour classer des sources d'incertitudes selon des applications particulières, et ainsi répondre à des préoccupations d'ordre pratique [RWi96, AOH04].

Une autre classification est basée sur les sources d'incertitudes présentes lors de la réalisation d'EPR [USN02] : les incertitudes de modèle, liées à l'adéquation des modèles pour représenter le monde réel ; les incertitudes paramétriques, liées aux valeurs d'entrée utilisées dans les modèles (à noter que la plupart des paramètres utilisés dans les EPR, tels les taux de défaillance ou les probabilités de défaillance à la demande, sont elles-mêmes des résultats issus de modèles, et n'ont généralement pas de signification physique) ; et les incertitudes de complétude, dues à des phénomènes ou à des relations significatives qui n'ont pas été considérés dans le modèle. Un exemple d'incertitude de complétude dans une EPR est l'omission de l'identification d'évènements qui pourraient impacter un scénario ou en initier un nouveau. Par nature, ce type d'incertitudes n'est pas vraiment quantifiable [JRe06], mais elles pourraient être réduites par l'utilisation de méthodes appropriées. En revanche, plusieurs approches mathématiques (probabilistes) ont été développées pour effectuer des analyses d'incertitudes liées aux paramètres : méthodes des moments [GAp77, ARu88], réseaux bayésiens [ECa99], méthodes de Monte Carlo [JHe06] ; ainsi que d'autres approches, parfois regroupées sous le terme de « théorie généralisée de l'information » [WOb04] : logique floue [DSi90, KMi90] et théorie des possibilités, théorie de l'évidence (ou « théorie de la croyance », « théorie de Dempster-Shafer »), et analyses par intervalles [JHe04]. À noter que la pertinence de théories alternatives à celles des probabilités, pour représenter des incertitudes, ne fait pas toujours l'unanimité [AOH04]. Les théories des probabilités sont alors considérées comme le moyen le plus rationnel [GAp90], et celles qui disposent des méthodes les plus répandues, acceptées, et développées [WOb04]. Dans le contexte des EPR, la plupart des approches citées précédemment ont été appliquées dans des méthodes par arbre de défaillance [GAp77, ARu88, ECa99, DSi90, KMi90], et l'utilisation de différentes sources de données pour l'attribution de valeurs aux paramètres des modèles a également été comparée et discutée [UHa08].

Les incertitudes de modèle peuvent prendre différentes formes [DGa93] : inadéquation du modèle conceptuel ; approximations et simplifications du modèle mathématique ; et erreurs numériques ou liées aux logiciels utilisés (ou à ses limites [NDu09]). Ces deux dernières relèvent plus de questions « techniques », et il ne sera donc fait qu'exclusivement référence à la première forme d'incertitudes de modèle dans la suite de ce mémoire de thèse. Contrairement aux incertitudes paramétriques, les

analyses d'incertitudes liées aux modèles sont moins répandues dans la littérature et, en outre, doivent faire face à des problématiques spécifiques. En effet, la plupart des modèles probabilistes exploités pour les EPR nécessitent de définir strictement les relations entre les évènements (par exemple, choix de transitions ou de portes logiques). Il est alors difficile d'analyser l'impact de ces incertitudes de modèle de manière cohérente, comme il est courant de le faire pour les paramètres, parce que ces contraintes sont de nature discrète, et les changer de façon aléatoire impliquerait bien souvent des structures irréalistes. En tant que première approche, un jeu de modèles basé sur des hypothèses alternatives plausibles peut être défini et combiné dans un méta-modèle, prenant en compte différents critères de vraisemblance [EZi96, JRe06]. Dans une méthode par arbre de défaillance, différents jeux de portes logiques (par exemple, de type « *k*-sur-*n* » [MRa02]) peuvent, par exemple, être considérés avec des probabilités d'adéquation respectives. Néanmoins, de par les résultats très différents qu'il est possible d'obtenir selon les portes logiques (plusieurs ordres de grandeur peuvent être observés entre des résultats obtenus pour une porte logique de type « *k*-sur-*n* » et de type « *(k+1)*-sur-*n* » [JKn02]), l'impact des probabilités attribuées à ces modèles alternatifs est souvent très important. Un niveau supplémentaire d'incertitude est alors ajouté [RWi96] et, comme une quantité importante d'information est, de plus, requise pour choisir ces derniers paramètres, les résultats finaux sont généralement très incertains. Une autre approche peut consister à définir un modèle de référence pour ensuite effectuer des analyses de sensibilité sur ses différentes hypothèses [EZi96]. L'utilisation de cette dernière option dans une méthode par arbre de défaillance rencontre cependant les mêmes difficultés que la première approche, de par les choix discrets des modèles alternatifs qui conduisent souvent à des résultats très différents. Enfin, une autre éventualité serait l'utilisation de la logique floue, par exemple en introduisant des « portes logiques floues » [HPa97], mais cela rendrait indisponible les critères mathématiques (par exemple, les variances) qui sont pertinents pour l'évaluation des incertitudes dans les résultats. Une contribution à cette problématique est proposée plus loin dans ce mémoire de thèse (Section III.3.1.2), afin de répondre à certaines particularités des capteurs-transmetteurs à fonctionnalités numériques (cf. Section I.3.3).

I.2.2. Systèmes Instrumentés de Sécurité

Nous avons vu dans la Section I.2.1.1 que parmi les principales tâches des EPR, figurent l'identification des *fonctions de sécurité* (qui entrent en jeu dans les scénarios d'accidents, cf. Figure I.2.1), et l'évaluation de leurs probabilités de réalisation et non-réalisation (par exemple en utilisant des arbres de défaillance, cf. Figure I.2.2). Les systèmes accomplissant ces fonctions sont les *barrières de sécurité*, et un type particulier de barrière inclut les *systèmes instrumentés de sécurité* (SIS). Les SIS et les fonctions de sécurité qu'ils réalisent sont le sujet de cette Section I.2.2.

I.2.2.1. Introduction aux fonctions de sécurité et à la norme CEI 61508

Un *système instrumenté de sécurité* (SIS) est communément constitué d'une chaîne de plusieurs éléments (ou groupe d'éléments) : capteurs-transmetteurs (par exemple, détection de gaz, contrôle de niveaux, mesure de pression ou de température) ; unités de traitement (par exemple, systèmes à relais, automates) ; et actionneurs (par exemple, vannes, pompes, alarmes). L'objectif d'un SIS est de réaliser une ou plusieurs *fonctions de sécurité* (cf. Section 1.2.1.1), c'est-à-dire des fonctions prévues pour assurer ou maintenir un état de sécurité d'équipements commandés (EUC, pour « *equipment under control* ») par rapport à un événement dangereux spécifique (par exemple, fuite, incendie, explosion). Face aux rôles critiques des SIS pour la maîtrise des risques technologiques,

en tant que *barrières de sécurité* (cf. Section I.1.1.2), leurs capacités à accomplir comme prévu leurs fonctions de sécurité doivent être étudiées et, dans le cadre d'une EPR, évaluées. Pour cela, des normes internationales dites de « sécurité fonctionnelle » ont été développées, notamment la principale référence européenne qui est la CEI 61508 sur la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité [IEC02, IEC10]. La première édition de cette norme date de la fin des années quatre-vingt-dix et début des années deux milles [IEC02], et la seconde édition vient d'être publiée en 2010 [IEC10].

La CEI 61508 adopte une approche basée sur le risque afin de proposer une méthode générale pour la spécification d'exigences de sécurité, et concerne tout le cycle de vie de sécurité des systèmes et du logiciel. De plus, cette norme à caractère générique sert de base à l'élaboration de normes de produit et d'application sectorielle. Parmi les normes d'application sectorielle, figure notamment la CEI 61511 [IEC04] pour les industries des procédés, et dont une équivalente américaine est l'ANSI/ISA S84.00.01-2004 [ISA04]. Des exemples de normes de produit sont la CEI 62061 [IEC05] pour les machines, et l'EN 50402 [ECE05] pour les systèmes de détection de gaz. La structure générale de la norme CEI 61508, avec les parties correspondantes (parmi les sept qui la composent), est comme suit :

1. définition des exigences globales de sécurité : concept, définition globale du domaine d'application, analyse des dangers et des risques, exigences globales de sécurité (Partie 1, Sections 7.1 à 7.5) ;
2. allocation des exigences de sécurité aux SIS (Partie 1, Section 7.6) ;
3. spécification des exigences de sécurité des SIS, afin d'obtenir la sécurité fonctionnelle requise (Partie 1, Section 7.10) ;
4. phase de réalisation, pour la conception des SIS en conformité avec la spécification des exigences de sécurité, concernant les systèmes (Partie 2) et les logiciels (Partie 3) ;
5. installation et mise en service, validation globale de la sécurité, avec les planifications associées (Partie 1, Sections 7.8, 7.9, 7.13, et 7.14) ;
6. exploitation, maintenance et réparation (avec la planification associée), modification et remise à niveau, mise hors service ou au rebut (Partie 1, Sections 7.7 et 7.15 à 7.17).

D'autres exigences concernent toutes les phases du cycle de vie de sécurité des SIS, au sujet de : la documentation (Partie 1, Section 5) ; la gestion de la sécurité fonctionnelle (Partie 1, Section 6) ; l'évaluation de la sécurité fonctionnelle (Partie 1, Section 8) ; et la vérification (Partie 1, Section 7.18). La Partie 4 donne les définitions et les abréviations utilisées dans la norme. Enfin, les autres parties sont informatives : la Partie 5 et la Partie 6 fournissent respectivement des lignes directrices pour l'application de la Partie 1 et des Parties 2 et 3 ; et la Partie 7 présente des techniques et des mesures.

Les deux sections suivantes présentent respectivement les exigences de sécurité des SIS (cf. point 3 de la liste précédente), ainsi que la conception des SIS (en excluant les aspects logiciels), (cf. point 4 de la liste précédente).

I.2.2.2. Exigences de sécurité des SIS, en accord avec la norme CEI 61508

En tant que notions fondamentales de la CEI 61508 se trouvent les exigences de sécurité des SIS (cf. Section I.2.2.1). Celles-ci concernent les *fonctions de sécurité* et les *niveaux d'intégrité de sécurité* associés. La spécification des exigences des fonctions de sécurité des SIS consiste à décrire toutes les fonctions de sécurité qui leurs sont allouées (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable), qui sont nécessaires pour obtenir la sécurité fonctionnelle requise. De plus, doivent être spécifiés : le temps de réponse requis pour la

réalisation des fonctions de sécurité ; les interfaces entre les SIS et les opérateurs ainsi que les autres systèmes ; les comportements requis des SIS en cas d'anomalies ; les modes de fonctionnement de l'EUC ; et toutes autres informations pertinentes susceptibles d'influencer la conception des SIS (cf. Section I.2.2.3). Une fonction de sécurité peut alors être sollicitée selon trois modes de fonctionnement [IEC10] : *faible sollicitation*, lorsqu'elle n'est réalisée que sur sollicitation (afin de faire passer l'EUC dans un état de sécurité spécifié), et où la fréquence des sollicitations n'est pas supérieure à une par an ; *sollicitation élevée*, lorsqu'elle n'est réalisée que sur sollicitation, et où la fréquence des sollicitations est supérieure à une par an ; et *continu*, lorsqu'elle maintient l'EUC dans un état de sécurité en fonctionnement normal (à noter que cette classification diffère de celle de la précédente édition de la norme [IEC02]).

La probabilité pour qu'un SIS accomplisse de manière satisfaisante les fonctions de sécurité spécifiées (dans toutes les conditions énoncées et dans une période de temps spécifiée) est l'*intégrité de sécurité* [IEC10] (ce qui correspond en fait à la « disponibilité » du SIS, cf. Section I.3.2.1). L'intégrité de sécurité comprend : l'intégrité de sécurité du matériel, qui est relative aux *défaillances aléatoires du matériel*, c'est-à-dire survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel ; et l'intégrité de sécurité systématique, qui est relative aux *défaillances systématiques*, c'est-à-dire liées de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés [IEC10]. Pour chaque fonction de sécurité, une exigence relative à l'intégrité de sécurité cible est allouée (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable). Les intégrités de sécurité sont alors classées selon quatre niveaux discrets, nommés *niveaux d'intégrité de sécurité* (SIL, pour « *safety integrity levels* »), dont le niveau 4 possède le plus haut degré d'intégrité, et le niveau 1 le plus bas. Pour cela, un *objectif chiffré de défaillance* est spécifié selon le mode de sollicitation de la fonction de sécurité : *probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité* (PFD_{avg}, pour « *average probability of failure on demand* »), définie comme une indisponibilité moyenne (cf. Section I.3.2.1.), pour un mode de faible sollicitation ; et *fréquence moyenne d'une défaillance dangereuse par heure* (*PFH*, pour « *probability of failure per hour* »), exprimée par heure, (à noter qu'il y a ici une certaine incohérence entre la définition de l'intégrité de sécurité, qui est une probabilité, et cette dernière, qui est une fréquence), pour un mode de sollicitation élevé ou continu [IEC10] (ce dernier mode de fonctionnement a notamment été discuté dans la littérature [FIn10, JBu08]). Les correspondances entre les SIL et les objectifs chiffrés de défaillance sont données dans les Tableaux I.2.1 et I.2.2, selon le mode de sollicitation de la fonction de sécurité.

En plus du niveau d'intégrité requis pour chaque fonction de sécurité, avec l'objectif chiffré de défaillance correspondant, et du mode de fonctionnement (faible sollicitation, sollicitation élevée, continu) de chaque fonction de sécurité, la spécification des exigences sur l'intégrité de sécurité des SIS doit comprendre : le cycle de service et la durée de vie requis ; les contraintes sur les essais périodiques (cf. Section I.2.2.3) ; les valeurs extrêmes des conditions environnementales des SIS ; les limites d'immunité électromagnétique ; et les contraintes relatives aux possibilités de défaillances de causes communes.

I.2.2.3. Conception des SIS, en accord avec la norme CEI 61508

Tableau I.2.1. Niveaux d'intégrité de sécurité (SIL) : objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à faible sollicitation (extrait de la norme CEI 61508 [IEC10])

niveau d'intégrité de sécurité (SIL)	*probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité* (PFD_{avg})
SIL 4	$10^{-5} \leq PFD_{avg} < 10^{-4}$
SIL 3	$10^{-4} \leq PFD_{avg} < 10^{-3}$
SIL 2	$10^{-3} \leq PFD_{avg} < 10^{-2}$
SIL 1	$10^{-2} \leq PFD_{avg} < 10^{-1}$

Tableau I.2.2. Niveaux d'intégrité de sécurité (SIL) : objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou continu (extrait de la norme CEI 61508 [IEC10])

niveau d'intégrité de sécurité (SIL)	*fréquence moyenne d'une défaillance dangereuse par heure* (*PFH*) [heure^{-1}]
SIL 4	$10^{-9} \leq PFH < 10^{-8}$
SIL 3	$10^{-8} \leq PFH < 10^{-7}$
SIL 2	$10^{-7} \leq PFH < 10^{-6}$
SIL 1	$10^{-6} \leq PFH < 10^{-5}$

Avant de débuter la phase de réalisation des SIS, les phases de définition, d'allocation, et de spécification des exigences de sécurité ont été menées. En particulier, les informations suivantes sont disponibles :

- les fonctions de sécurité allouées aux SIS ;
- le mode de fonctionnement de chaque fonction de sécurité ;
- les objectifs chiffrés de défaillance, avec les SIL correspondants.

L'objectif de la phase de réalisation est de concevoir des SIS en conformité avec la spécification des exigences de sécurité (cf. Section I.2.2.2). La phase de réalisation consiste en la spécification des exigences de conception ; la conception et le développement des SIS ; l'intégration ; les procédures d'installation, de mise en service, d'exploitation, et de maintenance ; et la validation (avec la planification associée). Dans cette section, ne sont présentés que la conception et le développement des SIS (en excluant ici les aspects logiciels), selon les exigences relatives à l'intégrité de sécurité du matériel (constituées des contraintes architecturales et de la quantification de l'effet des défaillances aléatoires du matériel) et à l'intégrité de sécurité systématique, ainsi que certaines exigences spécifiques. La conception des SIS est basée sur une décomposition en sous-systèmes qui comprennent un ou plusieurs éléments (capteurs-transmetteurs, unités de traitement, actionneurs) et qui, lorsqu'ils sont réunis, permettent la réalisation de la ou des fonctions de sécurité allouées.

Les *contraintes architecturales* (portant sur l'intégrité de sécurité du matériel), pour chaque élément (ou sous-système) du SIS, sont basées sur les trois critères suivants [IEC10] :

- la *tolérance aux anomalies du matériel* (*HFT*, pour « *hardware fault tolérance* ») de l'élément, qui est égale à *N* si *N+1* correspond au nombre minimal d'anomalies susceptibles de provoquer la perte de la fonction de sécurité ;
- la *proportion de défaillance en sécurité* (*SFF*, pour « *safe failure fraction* ») de l'élément, définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées (automatiquement par les essais de diagnostic en ligne), et des défaillances en sécurité et dangereuses (la méthode de calcul du *SFF* est présentée dans l'Annexe C de la Partie 2 de la norme) ;
- le *type d'élément*, qui est de « type A » si les modes de défaillance de tous ses composants sont biens définis, si son comportement dans des conditions d'anomalies peut être entièrement déterminé, et s'il existe des données de défaillance suffisamment fiables pour justifier des valeurs de taux de défaillance relatifs aux défaillances dangereuses ; et de « type B » si au moins l'une de ces conditions n'est pas vérifiée.

Le SIL maximal admissible pour une fonction de sécurité exécutée par un élément du SIS est alors donné dans les Tableaux I.2.3 et I.2.4, selon le type de l'élément. Pour un SIS constitué de plusieurs éléments, le SIL maximal admissible pour une fonction de sécurité allouée au SIS résulte alors de combinaisons de SIL, suivant des règles présentées dans la norme (Partie 2, Section 7.4.4.2).

Des travaux sur les contraintes architecturales des SIS, en accord avec la CEI 61508, ont été présentés dans la littérature [MLu09]. En particulier, la pertinence de l'utilisation du *SFF* comme critère de sécurité a souvent été remise en cause [YLa07, FIn06, JSi07a], tout comme les règles de combinaisons de SIL lorsqu'un SIS est constitué de plusieurs éléments [YLa08]. Une approche alternative a donc été introduite dans la seconde édition de la norme CEI 61508 [IEC10], qui est basée sur le retour d'exploitation et qui n'utilise ni le *SFF*, ni les règles de combinaisons de SIL. Une *HFT* minimale pour chaque élément (ou sous-système) du SIS exécutant une fonction de sécurité est alors définie, telle que donnée dans le Tableau I.2.5. De plus, une exigence supplémentaire est définie pour les éléments de « type B », qui consiste en une couverture de diagnostic (proportion de défaillances dangereuses détectées par les essais de diagnostic en ligne

Tableau I.2.3. Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type A » (extrait de la norme CEI 61508 [IEC10])

proportion de défaillances en sécurité (*SFF*) de l'élément	tolérance aux anomalies du matériel (*HFT*) de l'élément		
	HFT = 0	*HFT = 1*	*HFT = 2*
SFF < *60* %	SIL 1	SIL 2	SIL 3
60 % ≤ *SFF* < *90* %	SIL 2	SIL 3	SIL 4
90 % ≤ *SFF* < *99* %	SIL 3	SIL 4	SIL 4
SFF ≥ *99* %	SIL 3	SIL 4	SIL 4

Tableau I.2.4. Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type B » (extrait de la norme CEI 61508 [IEC10])

proportion de défaillances en sécurité (*SFF*) de l'élément	tolérance aux anomalies du matériel (*HFT*) de l'élément		
	HFT = 0	*HFT = 1*	*HFT = 2*
SFF < *60* %	.	SIL 1	SIL 2
60 % ≤ *SFF* < *90* %	SIL 1	SIL 2	SIL 3
90 % ≤ *SFF* < *99* %	SIL 2	SIL 3	SIL 4
SFF ≥ *99* %	SIL 3	SIL 4	SIL 4

Tableau I.2.5. Tolérance minimale aux anomalies du matériel pour chaque élément (ou sous-système) exécutant une fonction de sécurité d'un SIL spécifié, pour une approche basée sur le retour d'exploitation (d'après la norme CEI 61508 [IEC10])

niveau d'intégrité de sécurité (SIL)	tolérance minimale[a] aux anomalies du matériel (*HFT*)
SIL 4	*HFT = 2*
SIL 3	*HFT = 1*
SIL 2	*HFT = 0* ou *1*[b]
SIL 1	*HFT = 0*

[a]Pour des éléments de « type A », il est possible, dans certains cas, d'avoir des *HFT* minimales plus faibles si cela est justifié du point de vue de la sécurité (cf. CEI 61508, Partie 2, Section 7.4.4.3.2).

[b]Pour cette ligne, *HFT = 0* pour une fonction de sécurité en mode de fonctionnement à faible sollicitation, et *HFT = 1* pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou continu. Les autres lignes sont indépendantes du mode de fonctionnement de la fonction de sécurité.

automatiques [IEC10], dont la méthode de calcul est présentée dans l'Annexe C de la Partie 2 de la norme) d'au moins *60* %. Enfin, en utilisant cette approche, les données de fiabilité utilisées pour quantifier l'effet des défaillances aléatoires du matériel (cf. paragraphe suivant) doivent être [IEC10] : basées sur les retours d'exploitations ; basées sur les données recueillies conformément à des normes internationales ; évaluées selon la quantité de retours d'informations d'exploitation, des jugements d'experts, et la réalisation d'essais spécifiques si nécessaire ; de manière à estimer la moyenne et le niveau d'incertitude de chaque paramètre de fiabilité utilisé dans les calculs.

La *quantification de l'effet de défaillances aléatoires du matériel* permet d'obtenir l'intégrité de sécurité du SIS due aux défaillances aléatoires du matériel. Cette dernière doit être inférieure ou égale à l'objectif chiffré de défaillance (cf. Section I.2.2.2 et les Tableaux I.2.1 et I.2.2), (avec, de plus, une certitude supérieure à *90* % lorsque l'approche basée sur le retour d'exploitation est utilisée). Les exigences sur cette quantification consistent en une liste de paramètres à prendre en compte [IEC10] : l'architecture du système (en fonction de ses éléments) ; les taux de défaillance ; les causes communes de défaillance (dont plusieurs discussions, en rapport avec la norme CEI 61508, peuvent être trouvées dans la littérature [MLu07, PHo04, ASu99]) ; la couverture et les intervalles de temps des essais de diagnostic en ligne automatiques ; les intervalles de temps et l'efficacité des essais périodiques (essais destinés à détecter les défaillances dangereuses non détectées par les essais de diagnostic en ligne automatiques, le terme plus général de « tests de révision » sera également utilisé dans la suite de ce mémoire de thèse) ; les temps de réparation ; et l'effet d'erreurs humaines aléatoires (dont quelques discussions, en rapport avec la norme CEI 61508, peuvent aussi être trouvées dans la littérature [MSc10]). À noter que d'autres critères, bien que pertinents pour la sécurité comme les déclenchements intempestifs [MLu08a], ne sont quant à eux pas mentionnés dans cette liste. Certaines méthodes permettant cette quantification sont mentionnées (équations simplifiées, diagrammes de fiabilité, arbres de défaillance, chaînes de Markov, réseaux de Petri), uniquement à titre informatif, et sont présentées dans la Partie 6 de la norme. Plusieurs d'entre elles ont été discutées et comparées dans la littérature [YDu08a, JSi07b, YDu08b, JBu05, ASu00b].

Afin d'éviter l'introduction de défaillances systématiques pendant la conception et le développement du SIS, la méthode de conception doit répondre à certaines exigences, notamment de transparence, de clarté et de précision, de documentation, de vérification et de validation, ainsi que des exigences de maintenance et d'essais. De plus, pour la maîtrise des anomalies systématiques, la conception doit avoir des caractéristiques telles que les SIS soient tolérants à certaines anomalies de conception, de contraintes environnementales, et d'erreurs d'opérateurs. Plusieurs techniques et mesures appropriées à cela figurent dans les Annexes A et B de la Partie 2 de la norme. Lorsque le SIS est au-delà de la phase de conception, une alternative à ces exigences consiste à justifier qu'il est « éprouvé par une utilisation antérieure ». Il s'agit alors de démontrer que, sur la base d'une analyse de l'expérience d'exploitation pour une configuration spécifique d'un élément, la probabilité d'anomalies systématiques dangereuses est suffisamment faible pour que chaque fonction de sécurité qui utilise l'élément puisse atteindre son niveau d'intégrité requis [IEC10]. De tels critères ont été présentés et discutés dans la littérature [IVB04].

Enfin, d'autres exigences sont relatives : au comportement du SIS lors de la détection d'une anomalie qui, d'une manière générale, doit déclencher des actions spécifiées pour obtenir ou maintenir un état de sécurité de l'EUC (par exemple, par un arrêt de sécurité) ; aux communications de données, notamment par la prise en compte (le cas échéant) des erreurs de transmission, des répétitions, des délais, etc. dans la quantification de l'effet de défaillances aléatoires du matériel ; ainsi qu'aux circuits intégrés à redondance sur puce (le cas échéant), telles que précisées par l'Annexe E de la Partie 2 de la norme.

I.3. NOUVELLES TECHNOLOGIES ET SÛRETÉ DE FONCTIONNEMENT : EXEMPLE DES « CAPTEURS-TRANSMETTEURS INTELLIGENTS »

Après avoir présenté les EPR et les SIS dans la Section I.2, nous nous intéressons maintenant plus particulièrement aux capteurs-transmetteurs qualifiés d' « intelligents », et notamment lorsqu'ils constituent des éléments de systèmes instrumentés de sécurité (généralement, les premiers éléments de la chaîne des SIS, c'est-à-dire ceux qui réalisent des fonctions de détection ou de mesure).

I.3.1. Des « Capteurs-Transmetteurs Intelligents » ?

I.3.1.1. Terminologie

Depuis les années quatre-vingt, le développement des microsystèmes électromécaniques (MEMS) a ouvert la révolution des systèmes à « intelligence embarquée » et « distribués ». Par exemple, les systèmes de capteurs sont maintenant capables de combiner l'acquisition de données à partir de grandeurs physiques ou chimiques, avec le traitement interne et autonome de celles-ci, afin d'obtenir directement les informations souhaitées. Un signal élaboré peut alors être transmis à des systèmes externes, sous une forme appropriée. Dans l'industrie des procédés, et d'après les normes internationales de la Commission Électrotechnique Internationale (CEI) [IEC99] et de la Société Internationale d'Automatisation (ISA) [ISA93], de tels systèmes sont alors plus justement qualifiés de « transmetteurs » (en anglais, « *transmitters* ») au lieu de « capteurs » (en anglais, « *sensors* »), bien que ce dernier soit plus communément utilisé. Dans ce mémoire de thèse, le terme de « capteurs-transmetteurs » sera alors utilisé.

En anglais, l'utilisation des termes « *smart* » (occasionnellement traduit en français par « futé ») et « *intelligent* » est également sujet à discussions. Généralement, un capteur est qualifié de « *smart* » (en anglais, utilisé le plus fréquemment dans l'expression « *smart sensor* ») s'il intègre des conditionnements de signaux et des fonctions de traitement, effectués à l'aide de microprocesseurs embarqués [GSm95, JBr96, GMe94, CCo07]. Quant au terme « *intelligent* », pour des capteurs-transmetteurs, ce concept peut faire référence aux capacités de connaître (par l'utilisation de capteurs), de s'adapter aux situations (par l'utilisation d'unités de traitement et d'unités actives), et de communiquer [CIA87]. (Ces caractéristiques constituent la trame de l'architecture matérielle présentées dans la Section I.3.1.2.) En plus d'être « *smart* », un capteur-transmetteur est ainsi qualifié d' « *intelligent* » selon des fonctionnalités supplémentaires, impliquées dans le fonctionnement du système auquel il appartient [CIA05], telles que la capacité à modifier son comportement interne afin d'optimiser la collecte des données, et de les communiquer en réponse à un système hôte [JBr96]. En particulier, un « capteur-transmetteur intelligent » (CTI) dispose d'une communication bidirectionnelle avec des systèmes extérieurs et des opérateurs humains, pour transmettre des résultats de mesure et des informations de diagnostic, et recevoir et traiter des commandes externes [IEC06]. Cependant, cette distinction entre « *smart* » et « *intelligent* » n'est pas une règle universelle [CIA05], et ces termes sont souvent indifféremment utilisés [GMe94, HYa96, HSc94]. Dans la littérature scientifique française, seul le terme « intelligent » semble avoir été admis. En pratique, un capteur-transmetteur est communément qualifié d' « intelligent » simplement s'il possède certaines fonctionnalités relativement avancées (ou innovantes), notamment celles permises par les technologies numériques (cf. Section I.3.1.3).

Dans ce mémoire de thèse, nous préférerons ainsi utiliser le terme de « capteur-transmetteur à fonctionnalités numériques » que nous pensons plus approprié aux travaux qui sont présentés dans la suite. En accord avec le langage usuel, « capteur-transmetteur intelligent » (CTI) sera cependant utilisé comme synonyme.

I.3.1.2. Architecture matérielle

L'architecture matérielle d'un CTI, en accord avec la norme CEI 60770-3 sur les CTI utilisés dans les systèmes de contrôle pour les industries des procédés [IEC06], est décrite sur la Figure I.3.1.

Le sous-système *capteur* inclut : des transducteurs principaux qui convertissent des grandeurs physiques, chimiques, ou biologiques, à mesurer (les mesurandes), en signaux électriques ; des transducteurs auxiliaires qui font de même pour des facteurs d'influence (quantités qui ont un effet sur l'évaluation du mesurande, par exemple, température, pression, poussières, « gaz poisons ») ; des conditionneurs de signaux (multiplexeurs, amplificateurs, filtres, convertisseurs) ; des unités actives (par exemple, des commutateurs), qui peuvent servir à l'exécution de certaines fonctionnalités (cf. Section I.3.1.3) ; et des mémoires, qui permettent de stocker certaines caractéristiques de ce sous-système (par exemple, identification, paramètres métrologiques), pour être utilisées par le sous-système de *traitement des données*.

Le sous-système de *traitement des données* constitue la « partie intelligente » du capteur-transmetteur. Il effectue les traitements des données issues des sous-systèmes *capteur* et de *communication*, exécute les calculs, et assure les diverses fonctionnalités du CTI (cf. Section I.3.1.3), en utilisant des microprocesseurs, des mémoires (par exemple, pour stocker des données métrologiques et fonctionnelles, dont la datation est permise par une horloge interne), et des logiciels.

Les sous-systèmes de *communication* assurent : la transmission des résultats de mesure qui peut se faire analogiquement (généralement, par un signal en 4-20 mA), en utilisant un convertisseur numérique-analogique, ou numériquement (par exemple, via des réseaux de terrain [CIA05]) ; la transmission d'informations de diagnostic (par exemple, degré de confiance dans les résultats de mesure, état fonctionnel du CTI) à des systèmes extérieurs et à des opérateurs humains, en utilisant des câblages particuliers (par exemple, des réseaux de terrain) ou non (par exemple, via un signal analogique étendue en 0-24 mA, la technologie HART [HAR99], le courant porteur en ligne (CPL), ou une communication sans-fil). Afin de standardiser les interfaces de communication numérique, certains référentiels spécifiques ont été développés [OMG03, IEE07]. Enfin, des interfaces avec des systèmes extérieurs et des opérateurs humains permettent au capteur-transmetteur de recevoir des informations (par exemple, des résultats de mesure et des informations de diagnostic issus de systèmes extérieurs) et des commandes.

I.3.1.3. Fonctionnalités

Les nouvelles technologies, et en particulier l'utilisation du numérique, ont rendu disponibles des fonctionnalités innovantes au sein des capteurs-transmetteurs, alors communément qualifiés d' « intelligents » (cf. Section I.3.1.1). La *correction des erreurs de mesure*, l'*auto-ajustage*, l'*autodiagnostic*, la *reconfiguration en ligne*, et la *communication numérique et bidirectionnelle*,

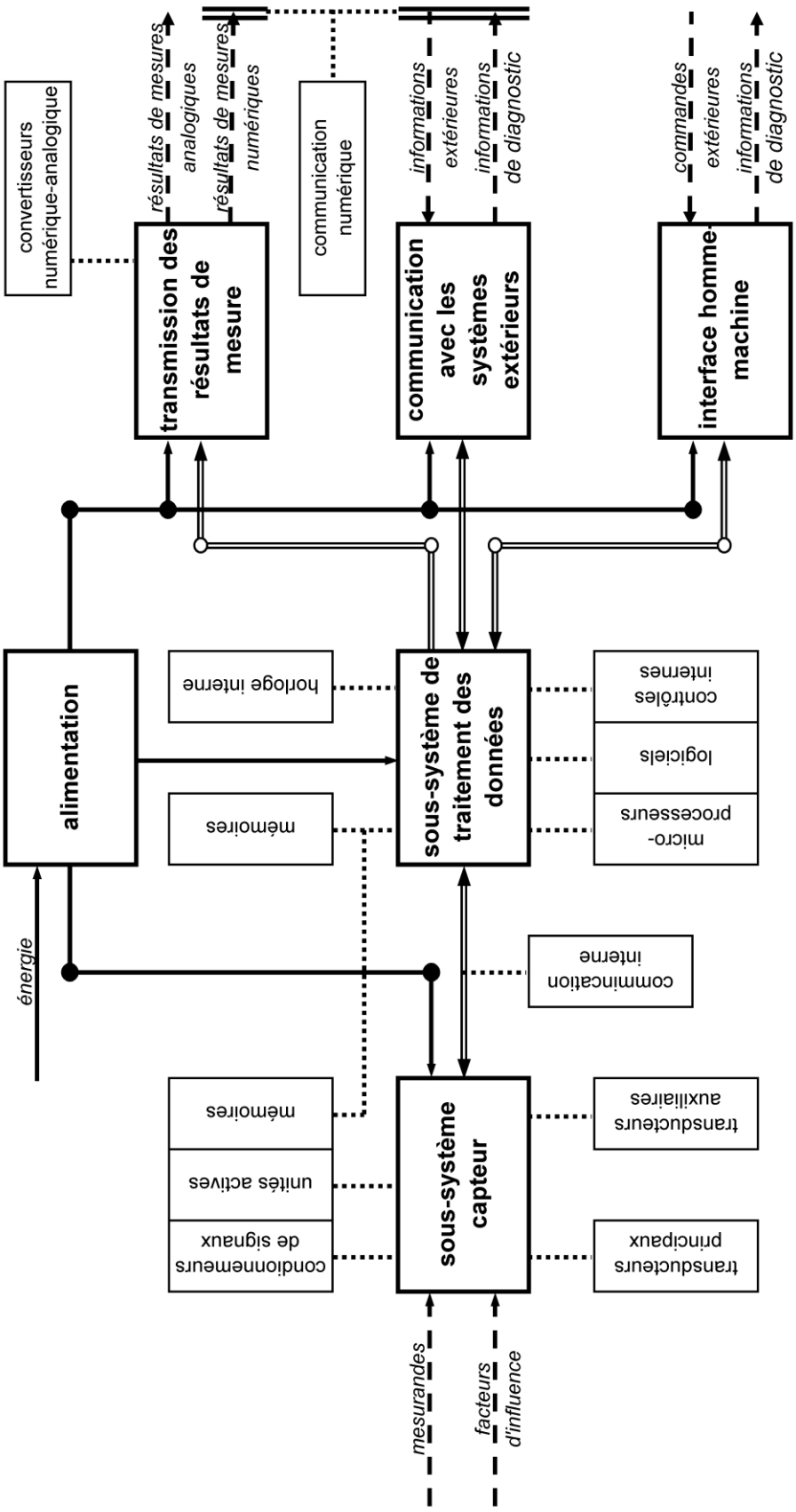

Figure I.3.1. Architecture matérielle d'un « capteur-transmetteur intelligent » (CTI)

sont présentées dans cette section. Celles-ci jouent, directement ou indirectement, un rôle dans les fonctions génériques d'un CTI, telles que décrites par M. Robert *et al.* [MRo93] : mesurer, configurer, valider, et communiquer. Elles contribuent ainsi à l'objectif principal du CTI qui est de fournir une mesure validée [MRo93].

Parmi les fonctionnalités les plus répandues, se trouve la *correction des erreurs de mesure* [GSm95, GMe94]. En utilisant des transducteurs auxiliaires et des contrôles internes, il est possible de corriger numériquement les résultats de mesure en fonction des grandeurs d'influence. De plus, le stockage de données métrologiques et fonctionnelles, avec datation, peut être utilisé pour corriger la linéarité, des dérives, et éventuellement pour remplacer certains résultats manquants ou aberrants. Enfin, des filtres numériques peuvent permettre d'atténuer certains bruits.

L'*auto-ajustage* est le procédé par lequel un capteur-transmetteur ou un groupe de capteurs-transmetteurs se met, de par lui-même, en conformité avec une fonction de transfert définie lors de l'étalonnage, afin de faire correspondre ses résultats de mesure avec les valeurs des mesurandes [IEC06, GSm95]. Des unités actives (commutateurs) peuvent être utilisées pour appliquer en entrée du CTI des signaux connus, puis des procédures permettent d'ajuster numériquement des paramètres internes (par exemple, biais, coefficients multiplicateurs), de façon à faire correspondre les résultats de sortie avec ceux escomptés. Par exemple, des ajustements du zéro, du gain, de la linéarité, et de la température (facteur d'influence répandue, et souvent aisé à mesurer), peuvent ainsi être effectués de façon autonome [ATa95]. Lorsque des CTI sont redondants, des auto-ajustages peuvent également être mis en place par comparaison des résultats de mesure ou d'autres informations.

Les *autodiagnostics* peuvent exploiter des procédures similaires de comparaison de résultats avec ceux escomptés, lorsque l'on applique des signaux ou des données d'entrée appropriées (par exemple, pour des connexions, des calculs, des traitements de données, des temps de réponse). Des paramètres internes (par exemple, température de l'électronique, puissance d'alimentation) et externes (facteurs d'influence) peuvent être surveillés afin de vérifier que le CTI se trouve dans des conditions acceptables. Certains composants disposent également de leurs propres modules de détection de défauts (ou « anomalies », cf. Section I.3.2.1). Ces données peuvent ensuite être utilisées dans des techniques de détection et d'isolation des défauts [GTi00, DMa95] (en anglais, « *fault detection and isolation* » (FDI)). À partir de ces résultats, la validation consiste à confirmer ou non la pertinence des informations transmises par le CTI, ou au minimum, à évaluer un degré de confiance associé. Différents niveaux de validation existent [MSt05, CIA05] : validation technologique (vérification des ressources physiques) ; validation fonctionnelle (vérification de la cohérence des données) ; et validation opérationnelle (par rapport au système de contrôle). Un CTI est alors potentiellement capable de transmettre des informations de diagnostic sur ses résultats mesures (grandeurs qualitatives ou symboliques [MSt05], incertitudes de mesure [GTi00], indices de validité [AMo01]), et sur son état fonctionnel [IEC06].

La *reconfiguration en ligne* est une autre fonctionnalité qui peut bénéficier des informations de diagnostic. Certaines caractéristiques du capteur peuvent être modifiées en temps réel, permettant par exemple de répondre à des exigences métrologiques (réglages) : adaptation de la plage de mesure et de la fréquence d'acquisition des données [GMe94], en fonction de l'évolution du phénomène observé et des facteurs d'influence. La reconfiguration peut également avoir des objectifs fonctionnels : gestion optimale des ressources et des fréquences de transmission des données. De plus, des techniques de tolérance aux défauts (en anglais, « *fault tolerant control* » (FTC)) peuvent être intégrées. Elles consistent à maintenir les aptitudes du CTI en présence de conditions anormales (défauts de composants, erreurs logicielles). Ses performances peuvent alors

être dégradées mais, à l'échelle du système, les défauts ne doivent pas conduire à une défaillance [MBl97]. Face à des défauts mineurs, il est possible d'effectuer des compensations numériques (accommodation), de la même façon que pour la correction des erreurs de mesure ; le cas échéant, une modification fonctionnelle (restructuration), par exemple en exploitant des ressources redondantes, permet de maintenir un état fonctionnel acceptable du CTI. Des critères de fiabilité peuvent alors être inclus dans les choix optimaux de ces reconfigurations [FGu06].

Enfin, la *communication numérique et bidirectionnelle* [IEC06, CIA05] permet à la fois de transmettre plusieurs types d'informations (par exemple, résultats de mesure, informations de diagnostic) ; et de recevoir des informations et des commandes issues de systèmes extérieurs ou d'opérateurs humains.

I.3.2. Sûreté de Fonctionnement et « Capteurs-Transmetteurs Intelligents »

I.3.2.1. Sûreté de fonctionnement

La *sûreté de fonctionnement* (en anglais, « *dependability* ») est définie par la Commission Électrotechnique Internationale (CEI) comme l'ensemble des propriétés qui décrivent la disponibilité et les facteurs qui la conditionne : fiabilité, maintenabilité et logistique de maintenance [IEC90]. Afin de compléter cette définition, précisons que la *disponibilité* (en anglais, « *availability* ») est l'aptitude d'une entité à être en état d'accomplir une fonction requise, dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée [IEC90]. Quantitativement, la disponibilité d'une entité à un instant donné s'exprime par la probabilité suivante :

$$A(t) = P[\text{l'entité est en état d'accomplir la fonction requise au temps } t] \quad \text{[I.3.1]}$$

et la disponibilité moyenne peut s'exprimer par [MRa02] :

$$A_{avg} = MUT / (MUT + MDT) \quad \text{[I.3.2]}$$

où *MUT* (pour « *mean up time* ») est le temps moyen où l'entité est en état d'accomplir la fonction requise (temps moyen entre la mise en état de l'entité et l'occurrence d'une défaillance), et *MDT* (pour « *mean down time* ») est le temps moyen où l'entité n'est pas en état d'accomplir la fonction requise (temps moyen de réparation, de remise en état, etc.). Enfin, lorsqu'il est question d'*indisponibilité*, cette dernière s'exprime au temps *t* par $U(t) = 1 – A(t)$, et en moyenne par $U_{avg} = 1 – A_{avg}$.

De plus, une *défaillance* (en anglais, « *failure* ») est définie comme la cessation de l'aptitude d'une entité (unité fonctionnelle) à accomplir une fonction requise (ou à fonctionner comme prévu) [IEC90, IEC10] ; et nous définirons ici un *défaut* (en anglais, « *fault* »), (utilisé comme synonyme d' « *anomalie* » telle que définie par la norme CEI 61508), comme une condition anormale qui peut entraîner une réduction de capacité, ou la perte de capacité, d'une entité (unité fonctionnelle) à accomplir une fonction requise [IEC10]. Ainsi défini, le terme de *défaut* correspond à une définition plus générale donnée par une autre norme de la CEI [IEC90] (pour les réseaux d'énergie électrique) : évènement imprévu ou défectuosité d'une entité qui peut donner lieu à une défaillance. (À noter que, dans certaines références et y compris issues de la CEI, le terme anglais de « *fault* » est également traduit en français par le terme de « panne », qui correspond alors à une définition contradictoire.)

Pour résumer, nous pourrions donc caractériser la sûreté de fonctionnement comme étant l'étude des défauts et des défaillances, par l'intermédiaire du critère principal qui est la disponibilité. La disponibilité dépend quant à elle de la fiabilité, et de la maintenabilité et logistique de maintenance (cf. Section I.3.2.2 et I.3.2.3). Souvent, la sécurité (cf. Section I.3.2.4) est, de plus, incluse dans les facteurs de la sûreté de fonctionnement, formant ainsi le concept de FMDS (fiabilité, maintenabilité, disponibilité, sécurité), (en anglais, RAMS pour « *reliability, availability, maintainability, safety* »).

Dans les sections suivantes, des discussions sur la sûreté de fonctionnement des CTI sont ainsi proposées au regard des attributs que sont la fiabilité, la maintenabilité et logistique de maintenance, et la sécurité.

I.3.2.2. Fiabilité

La *fiabilité* (en anglais, « *reliability* ») est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné [IEC90]. Quantitativement, la fiabilité d'une entité à un instant donné s'exprime par la probabilité suivante :

$R(t) = P[$l'entité reste en état d'accomplir la fonction requise jusqu'au temps $t]$ [I.3.3]

(En général, on suppose que l'entité est en état d'accomplir la fonction requise au temps initial.)

La fiabilité d'un CTI peut tirer avantage de certaines fonctionnalités numériques lorsque, par exemple, des corrections d'erreurs de mesure et des auto-ajustages permettent de prévenir l'occurrence de dérives ou d'autres défauts ou défaillances qui apparaissent avec la durée. De plus, certains défauts peuvent en partie être compensés par l'utilisation de techniques de tolérance aux défauts (reconfigurations). Lorsque des défaillances se produisent au bout d'une échéance quasi-déterministe (par exemple, épuisements de ressources), on évoquera alors plus justement des questions de *durabilité* (aptitude d'une entité à accomplir une fonction requise, dans des conditions données d'emploi et de maintenance, jusqu'à ce qu'un état limite soit atteint [IEC90]) qui peut, elle aussi, bénéficier de reconfigurations fonctionnelles en ligne du CTI (par exemple, pour une gestion optimisée des ressources). La communication numérique est, quant à elle, souvent considérée comme plus fiable que l'analogique. En revanche, la plus grande quantité d'électronique, d'unités programmées, et de logiciels, (nécessaires aux traitements des données, aux calculs, à l'exécution des fonctionnalités, à la communication, etc.), implique de nouvelles causes et de nouveaux modes de défaillance qui sont généralement difficiles à connaître et à appréhender. De plus, chaque défaut ou défaillance peut affecter plusieurs fonctions du CTI, ainsi que plusieurs informations transmises par celui-ci. Enfin, la communication numérique fait encore l'objet de plusieurs interrogations au regard de la fiabilité, notamment face aux causes communes de défaillance.

I.3.2.3. Maintenabilité et logistique de maintenance

La *maintenabilité* (en anglais, « *maintainability* ») est l'aptitude d'une entité, (dans des conditions données), à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise (lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits) ; et la *logistique de maintenance* est l'aptitude d'une organisation de maintenance à fournir sur demande, (dans des conditions données), les moyens nécessaires à la maintenance d'une entité, (conformément à une politique de maintenance donnée) [IEC90].

La maintenabilité et la logistique de maintenance d'un CTI peut alors bénéficier d'informations collectées par le CTI (autodiagnostics) et surveillées dans le temps (par exemple, des dérives, des

valeurs de facteurs d'influence, des dépassements de seuils, l'énergie d'alimentation, l'occurrence de défauts et défaillances avec les circonstances correspondantes), notamment pour favoriser la maintenance préventive (par exemple, par la prédiction de certaines défaillances). De plus, la communication numérique et des reconfigurations en ligne peuvent rendre certaines opérations de maintenance simplifiées et plus efficaces, notamment grâce à une centralisation de certaines informations, une réduction des câblages, et une interface plus complète entre les CTI et les opérateurs humains. Dans de nombreux cas, une certaine expertise est cependant nécessaire pour maintenir de tels systèmes devenus plus complexes.

I.3.2.4. Sécurité

Nous définirons ici la *sécurité* (en anglais, « *safety* ») comme l'aptitude d'une entité à prévenir l'occurrence d'évènements dangereux (événements susceptibles de conduire à des atteintes à la santé des personnes, à l'environnement, ou aux biens [IEC10]), ou à réduire les conséquences de tels évènements sur les personnes, l'environnement, ou les biens.

Les bénéfices apportés à la sécurité, par les fonctionnalités numériques au sein des CTI, résident principalement dans les capacités plus complètes d'autodiagnostics, qui permettent ainsi une meilleure détection des défauts et défaillances. De plus, des états « sûrs » peuvent être définis avec plus de détails et obtenus plus justement par des reconfigurations. La centralisation de certaines informations, permise par la communication numérique, peut également contribuer à une maîtrise des risques plus efficace. En revanche, les capteurs-transmetteurs deviennent de plus en plus des « boites noires », qu'il convient donc d'évaluer avec des outils appropriés.

I.3.3. Évaluer des « Capteurs-Transmetteurs Intelligents » : Enjeux et Difficultés

L'utilisation de CTI pour des activités industrielles permet d'apporter certains avantages pratiques : une meilleure exactitude des résultats de mesure [GMe94, PBi05], par des corrections d'erreurs de mesure (pour les erreurs aléatoires), et des auto-ajustages (pour les erreurs systématiques) ; des réductions de coûts [CIA87, GSm95, EXE01], en termes de câblage, d'installation et de maintenance, bien que les coûts directs soient souvent plus élevés de par l'électronique et les logiciels supplémentaires ; ainsi que des facilités d'utilisation [FBe95, GMi01, EXE01]. Cela explique l'utilisation accrue de ces systèmes dans plusieurs secteurs d'activité, y compris le nucléaire et l'industrie des procédés [GSm95, FBe95, PBi05]. Cependant, les particularités des CTI soulèvent quelques problématiques pour la sûreté de fonctionnement (cf. Section I.3.2).

Lorsque des CTI font partie de systèmes relatifs à la sécurité, leur sûreté de fonctionnement doit être évaluée, par exemple en accord avec les normes de sécurité fonctionnelle CEI 61508 [IEC10] et CEI61511 [IEC04] (cf. Section I.2.2). Un CTI est alors considéré comme un système « complexe » (et de « type B », cf. Section I.2.2.3) au regard de la CEI 61508 [FBr09b], et « électronique programmable » (PE, pour « *programmable electronic* ») au regard de la CEI 61511 (car « basé sur les technologies de l'informatique » [IEC04]). Cela implique des exigences plus contraignantes, en particulier quant aux tolérances aux défauts (anomalies), (à noter que pour la CEI 61511, les Tableaux I.2.3 et I.2.4 diffèrent de ceux de la CEI 61508), et aux couvertures de diagnostic (cf. Section I.2.2.3). De plus, les CTI doivent être « protégés en écriture pour prévenir une modification

involontaire depuis un site distant, sauf si une revue de sécurité appropriée autorise l'utilisation de la lecture/écriture » [IEC04].

Les analyses de fiabilité des CTI sont alors nécessaires à la définition des intégrités de sécurité pour des systèmes relatifs à la sécurité (cf. Section I.2.2.2), mais peuvent également être utilisées afin de disposer de données pour mettre en place des fonctionnalités d'autodiagnostics et de validations [AMo01, MSt05], et de reconfiguration en ligne [FGu06] (cf. Section I.3.1.3), ainsi que pour la conception de réseaux de capteurs-transmetteurs [CBe04, MBh00, MBh08]. Du point de vue qualitatif, des analyses des modes de défaillance, de leurs effets, et de leurs criticités (AMDEC) relatives aux CTI peuvent être trouvées dans la littérature, par exemple au regard de la communication numérique [LCa04], des diagnostics [MGo99], et des causes communes de défaillance [MMe04]. Du point de vue quantitatif, des analyses de fiabilité relatives aux CTI se sont également concentrées sur certains aspects, notamment l'autodiagnostic [AMk08], et la communication numérique [PBa02, RGh06, RGh11]. En dehors de ces aspects particuliers, les évaluations de sûreté de fonctionnement relatives aux CTI considèrent généralement ces systèmes comme des « boites noires », et leurs fonctionnalités numériques ne sont alors pas explicitement prises en compte dans leur globalité.

Des analyses de fiabilité d'un CTI doivent répondre aux difficultés suivantes :

i. la complexité du système, liée aux nombreuses interactions à la fois entre les éléments matériels et les fonctions ;
ii. les comportements mal connus et difficiles à appréhender du système en cas de défauts ou de défaillances (en particulier de par la présence d'unités programmées et de logiciels) ;
iii. la multitude des informations transmises par le système (par exemple, résultats de mesure, informations de diagnostic), qui peuvent être erronées de façon nuancée (la nature des informations transmises étant souvent continue) et dépendante ;
iv. le peu de retour d'expérience disponible (qualitatif, sur les modes de défaillance, et quantitatif, sur les paramètres de fiabilité) de par la nature « nouvelle » des technologies utilisées.

Ces points rendent les analyses qualitatives comme les AMDEC difficilement exhaustives pour l'identification des modes de défaillance, face aux points ii et iv, et pour prendre en compte les combinaisons de défauts et de défaillances, face aux points i et iii. De plus, les modèles binaires de fiabilité (par exemple, diagrammes de fiabilité, arbres de défaillance) sont souvent inappropriés en l'état, en particulier à cause des points ii et iii. Enfin, les approches par transitions entre états (par exemple, chaînes de Markov, réseaux de Petri) doivent faire face à certaines difficultés dans la définition des états et des transitions de par les points i et ii.

De plus, lorsque des CTI constituent des éléments d'un système (par exemple, d'un SIS ou d'un système de contrôle-commande de processus), alors les évaluations de sûreté de fonctionnement doivent également répondre aux caractéristiques suivantes :

v. les CTI d'un même système interagissent par une communication numérique et bidirectionnelle, et certaines de leurs opérations (notamment par l'intermédiaire des fonctionnalités numériques) peuvent alors s'effectuer en « collaboration » ;
vi. de façon encore plus globale, la sûreté de fonctionnement d'un système intégrant des CTI est dépendante des interactions entre les CTI, entre les CTI et les autres éléments du système, ainsi que des interactions avec le processus contrôlé.

I.4. ORGANISATION DU MÉMOIRE DE THÈSE

Afin de répondre aux mieux aux problématiques soulevées dans ce chapitre, nous avons choisi d'aborder les travaux de thèse en trois thèmes, respectivement présentés dans les Chapitres II, III, et IV.

Avant de s'intéresser spécifiquement aux capteurs-transmetteurs à fonctionnalités numériques, le Chapitre II concerne plus généralement l'évaluation de la sûreté de fonctionnement des systèmes relatifs à la sécurité (en tant qu'éléments ou sous-systèmes de SIS). L'objectif de ce chapitre est double : contribuer au développement de modèles d'évaluation probabiliste des risques en accord avec l'interprétation subjective des probabilités (cf. Section I.2.1.2) ; et montrer les apports d'approches probabilistes pour l'évaluation des risques (notamment suite au cadre réglementaire français présenté dans la Section I.1.1.2). Sont ainsi présentés dans le Chapitre II : une approche dite « analytique » pour la quantification des effets des défaillances aléatoires du matériel (cf. Section I.2.2.3), avec une attention particulière portée sur les architectures des systèmes et les tests de révision ; et une méthodologie d'évaluation des taux de défaillance (paramètres requis pour la quantification des effets des défaillances aléatoires du matériel) en fonction des facteurs d'influence propres à chaque système. Bien que présentés indépendamment, ces deux travaux peuvent être utilisés conjointement (le second fournissant des données d'entrée pour le premier). Les apports de ceux-ci résident dans la proposition de modèles relativement simples à mettre en place, qui cherchent à refléter au mieux la gradation des risques, notamment en intégrant une plus grande quantité d'informations pertinentes (architectures des systèmes, tests de révision, facteurs d'influence). La mise en application de ces travaux sur des cas d'étude permet alors de montrer l'intérêt de ces approches dans la maîtrise des risques technologiques.

L'évaluation, plus spécifique, de la sûreté de fonctionnement des capteurs-transmetteurs à fonctionnalités numériques, en premier lieu considérés en tant que systèmes à part entière, est ensuite le sujet du Chapitre III. L'objectif de ce chapitre est alors de proposer des outils de modélisation et d'évaluation qui prennent en compte les particularités des CTI (cf. Section I.3.1), qui permettent d'apporter des éléments de réponse aux problématiques liées à la sûreté de fonctionnement de ces systèmes (cf. Section I.3.2), et qui puisse satisfaire aux enjeux et difficultés présentés dans la Section I.3.3. Tout d'abord, face à la complexité de ces systèmes, une méthode de modélisation est développée, qui représente les aspects matériels et fonctionnels, ainsi que les diverses interactions associées. Les défauts et défaillances sont également inclus, pour permettre d'effectuer des analyses de fiabilité sur la base du modèle proposé. En réponse aux comportements mal connus de ces système et difficiles à appréhender, des analyses de relations cherchent à évaluer les effets de n'importe quel défaut ou défaillance sur les éléments matériels et les fonctions du système. Les probabilités de dysfonctionnements et de modes de défaillance du système, définies sur la base des informations qu'il transmet, sont ensuite évaluées en tenant compte de ces relations. Enfin, des analyses d'incertitudes testent la robustesse des résultats obtenus face aux incertitudes liées aux paramètres (notamment dues au peu de retour d'expérience) et aux comportements mal connus du système. Un cas d'étude permet d'illustrer la mise en œuvre de ces approches.

Dans le Chapitre IV, les CTI sont ensuite intégrés à des systèmes de contrôle-commande (SCC), en tant qu'éléments de ce dernier, dont l'évaluation de la sûreté de fonctionnement constitue alors en une approche encore plus systémique. Tout en continuant de prendre en compte les particularités des CTI (cf. Section I.3.1), l'objectif de ce chapitre est alors de développer des modèles d'évaluation qui intègrent les interactions entre les CTI puis, dans un second temps, également les interactions avec les autres éléments du SCC, ainsi qu'avec le processus contrôlé (cf. Section I.3.3).

Une première partie du Chapitre IV permet d'introduire un système constitué de plusieurs CTI qui tirent avantage d'une communication numérique et bidirectionnelle pour s'échanger des informations et effectuer des opérations en « collaboration ». Des réseaux de Petri colorés et stochastiques sont alors utilisés pour modéliser et évaluer ce système où, pour ce premier exemple, seules les interactions entre les CTI ont été prises en compte. Dans une seconde partie du Chapitre IV, une approche plus formalisée a été développée afin de modéliser explicitement les états fonctionnels des éléments du système, le processus, les informations (notamment celles qui sont manipulées par les CTI), certains phénomènes de dégradation et de dérive, ainsi que l'ensemble des interactions associées. Cette approche de fiabilité dynamique est ensuite illustrée par un cas d'étude relativement complet.

Enfin, le Chapitre V présente des conclusions et des perspectives de l'ensemble de ces travaux de thèse ; le Chapitre VI regroupe les annexes où figurent les démonstrations de plusieurs des expressions mathématiques proposées dans les Chapitres II et III ; et le Chapitre VII présente les références bibliographiques citées tout au long de ce mémoire, ainsi que celles produites lors des travaux de thèse.

CHAPITRE II

SÛRETÉ DE FONCTIONNEMENT DE SYSTÈMES RELATIFS À LA SÉCURITÉ

Ce chapitre présente l'évaluation de la sûreté de fonctionnement de systèmes relatifs à la sécurité, en tant qu'éléments ou groupes d'éléments de systèmes instrumentés de sécurité. Les objectifs sont de contribuer au développement de modèles d'évaluations probabilistes des risques, et d'illustrer certains intérêts de ce type d'approches pour la maîtrise des risques technologiques.

La première section de ce chapitre propose des expressions pour l'évaluation des probabilités de défaillance à la sollicitation, généralisées aux systèmes d'architectures redondantes et avec l'inclusion de tests de révision partiels et complets. La seconde section développe une méthodologie d'évaluation des taux de défaillance en fonction des facteurs d'influence propres aux systèmes considérés. Ces deux parties sont présentées de façon indépendante, mais peuvent aisément être associées, la seconde fournissant des données d'entrée à la première.

Ce chapitre relate des travaux qui ont principalement été financés par un programme d'appui technique au Ministère de l'Écologie, faisant suite à des besoins exprimés en termes d'outils d'évaluations probabilistes. Le contexte est ainsi plus général que celui des capteurs-transmetteurs à fonctionnalités numériques, traité dans les chapitres suivants.

Les publications réalisées en lien avec les travaux de ce chapitre sont présentées dans la Section VII.2.1.

SOMMAIRE DU CHAPITRE II

II.1. PROBABILITÉS DE DÉFAILLANCE À LA SOLLICITATION DE SYSTÈMES RELATIFS À LA SÉCURITÉ

II.1.1. Probabilités de Défaillance et Tests de Révision Complets et Partiels

Dans le cadre d'une évaluation probabiliste des risques, les systèmes relatifs à la sécurité (en tant qu'éléments ou groupe d'éléments de systèmes instrumentés de sécurité) doivent être évalués, par exemple d'après la norme CEI 61508 [IEC10] (cf. Section I.2.2.1). Dans la présente Section II.1, nous nous focaliserons sur la *quantification de l'effet des défaillances aléatoires du matériel* qui, dans la phase de réalisation des SIS suivant la CEI 61508, permet d'obtenir l'*intégrité de sécurité* du système relative aux défaillances aléatoires du matériel (cf. Section 1.2.2.3). De plus, seul le mode de fonctionnement à *faible sollicitation* (la fonction de sécurité exécutée par le système n'est réalisée que sur sollicitation, et pas plus d'une fois par an) est considéré, et le critère à évaluer est donc la *probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité* (*PFD_{avg}*, pour « *average probability of failure on demand* »), (cf. Section I.2.2.2). Rappelons que ce critère permet de vérifier un *niveau d'intégrité de sécurité* (SIL, pour « *safety integrity level* ») maximal admissible pour une fonction de sécurité (cf. Tableau I.2.1), mais n'est pas un critère suffisant.

La CEI 61508 définit la *probabilité de défaillance dangereuse en cas de sollicitation* (*PFD*, pour « *probability of failure on demand* ») comme l'indisponibilité d'un système pour réaliser la fonction de sécurité spécifiée ; et *PFD_{avg}* comme la moyenne de cette indisponibilité [IEC10]. Dans la suite, seules les défaillances qualifiées de « dangereuses » (défaillances qui empêchent le fonctionnement nécessaire de la fonction de sécurité, ou qui diminuent la probabilité que la fonction de sécurité fonctionne correctement lorsque c'est nécessaire [IEC10]) sont considérées, tel que précisé dans les hypothèses ci-après (cf. Section II.1.2.1), et l'adjectif « dangereuse » est donc omis. De plus, le pluriel est utilisé pour évoquer les *probabilités de défaillance à la sollicitation* (PFD), qui regroupent les critères d'*indisponibilité à un instant donnée* (notée *U(t)* pour l'indisponibilité au temps *t*) et ceux d'*indisponibilité moyenne* (qui incluent *PFD_{avg}*, l'indisponibilité moyenne sur une période d'essais périodiques efficaces à *100*%).

En accord avec la CEI 61508, et les hypothèses précisées ci-après (cf. Section II.1.2.1), les paramètres suivants doivent être pris en compte pour l'évaluation des PFD : l'architecture du système (redondance de ses éléments) ; les taux de défaillance des éléments du système ; les intervalles de temps et les efficacités des tests de révision (ici, le terme « test de révision » est préféré à celui plus général d' « essais périodiques », car le caractère « périodique » n'est pas indispensable à l'application des modèles développées ci-après). Un test de révision est *partiel* s'il n'est pas parfait, c'est-à-dire qu'il est capable de détecter uniquement certaines défaillances des éléments du système, et laisse les autres latentes. Des inspections visuelles et des sollicitations partielles (par exemple, inspection visuel d'un détecteur de flamme ou de gaz [PHo95], actionnement d'une vanne jusqu'à mi-course [ASu00a, MLu08b]) sont des exemples de tests partiels. Lorsqu'un test de révision est parfait (efficace à *100*%), il est alors qualifié de *complet*, et se rapporte à l'ensemble des actions d'inspection et de maintenance à la suite desquelles le système est restauré dans un état qui peut être considéré comme « aussi bon que neuf ». Bien que les tests partiels soient moins efficaces, ils peuvent être préférés aux tests complets pour plusieurs raisons :

- les tests complets sont généralement physiques (par exemple, stimulation des éléments sensibles d'un capteur), coûteux, et requièrent un temps d'exécution éventuellement long, ils peuvent alors parfois être remplacés par des tests entièrement électroniques (par exemple, des simulations électroniques de sollicitations), mais qui ne couvrent pas toutes les défaillances possibles ;
- les tests complets nécessitent souvent des arrêts de production (par exemple, coupure d'une alimentation, arrêt d'un flux par une vanne de sécurité), qui peuvent être jugés inacceptables pour les industriels, et des tests partiels (par exemple, fermeture au quart de tour d'une vanne) peuvent alors être préférés ;
- certains dispositifs de sécurité ne peuvent pas être testés complètement sans dégradations ou destructions de ceux-ci (par exemple, des dispositifs fonctionnant par « rupture ») ;
- uniquement des tests exécutés dans des conditions réelles peuvent prétendre être complets et, dans plusieurs cas, pourraient alors provoquer plus de situations de danger que de prévention (par exemple, détection d'incendie, de gaz toxiques, ou de surpression).

Plusieurs évaluations de PFD ont été proposées selon les méthodes mentionnées (à titre informatif) dans la CEI 61508 : équations simplifiées [ASu00a, LOl10, JVa11], diagrammes de fiabilité [HGu07], arbres de défaillance [YDu08b], approches markoviennes [TZh03, JBu06, JBu05, YDu08a, YLa08], et réseaux de Petri [JSi07b, YDu08a, YDu08b, AKl10], mais sans intégrer de tests partiels (à l'exception de la référence citée pour les arbres de défaillance [YDu08b]). L'utilisation de ce type de tests peut être assimilée à une certaine forme de maintenance préventive imparfaite, dont des états de l'art ont été présentées dans la littérature [HPh96]. Par exemple, certaines approches définissent une probabilité (constante) qu'une maintenance préventive soit parfaite ou imparfaite [MBr83, TNa87]. Plus spécifiquement, des probabilités de non-détection de défaillances lors de tests ont également été considérées pour exprimer des PFD sous formes analytiques, mais uniquement pour des systèmes sans redondance [PHo95, MLu08b, FBa02a], ou d'architecture parallèle [ATo09]. Pour des cas plus généraux, et de façon plus flexible, les arbres de défaillance permettent d'intégrer des tests partiels [YDu08b], ainsi que des approches markoviennes « étendues » [JBu01, GLe06, TZh08, MKu08] (de type « multi-phases », afin de prendre en compte la nature déterministe des instants de tests périodiques). En particulier, l'effet de ces tests sur les PFD d'un système a ainsi été étudié par J.V. Bukowski [JBu09]. Enfin, il convient de noter que dans toutes ces références citées, les tests partiels sont toujours considérés comme périodiques.

Dans cette présente Section II.1, une approche communément qualifiée d' « analytique » a été choisie, afin de formuler des expressions générales sous une forme relativement simple, et aisées à calculer sans l'aide d'outils particuliers. Celles-ci sont proposées pour évaluer les PFD de systèmes d'architecture *M*oo*N* (*k*-sur-*n* [MRa02], avec $k = M$ et $n = N$), constitués d'éléments homogènes (dont les taux de défaillance sont identiques), et soumis à des tests de révision partiels et complets. Les tests partiels peuvent être exécutés à différents instants (périodiques ou non), jusqu'au test complet. La Section II.1.2 présente les hypothèses, les notations, et les expressions. Un cas d'étude est ensuite présenté dans la Section II.1.3, pour des estimations paramétriques, des évaluations de PFD, et une optimisation de la répartition des tests partiels.

II.1.2. Expressions Générales des Probabilités de Défaillance à la Sollicitation

II.1.2.1. Hypothèses générales

Les hypothèses suivantes sont considérées dans les Sections II.1.2 et II.1.3 :

- toutes les défaillances prises en compte sont « dangereuses » et uniquement détectées par des tests de révision (partiels ou complets) ;
- le système est constitué de N éléments qui sont indépendants (en particulier, les causes communes de défaillance ne sont pas considérées), et qui ont des taux de défaillance constants et identiques ;
- le système est d'architecture *M*oo*N*, c'est-à-dire qu'il est divisé en N éléments, et qu'il est capable d'accomplir de manière satisfaisante la fonction de sécurité spécifiée si et seulement si M de ces éléments (n'importe lesquels) sont opérants (système « *M*-sur-*N* », et en anglais, « *M-out-of-N* ») ;
- les N éléments du système sont opérants (dans des conditions « comme neuves ») au temps initial $t_0 = 0$;
- les tests partiels sont capables de détecter uniquement certaines défaillances spécifiques de chaque élément du système ;
- les tests complets sont capables de détecter toutes les défaillances de chaque élément du système ;
- tous les éléments du système sont révisés simultanément (approximation qui peut se justifier par la durée des tests de révision très petites par rapport à l'intervalle de temps entre ces tests) lors de chaque test de révision (partiel ou complet) ;
- lorsqu'une défaillance est détectée par un test partiel ou complet, elle est réparée immédiatement ; lors des actions de révision et de maintenance, des mesures sont prises afin de maintenir un état de sécurité, de telle sorte que les durées des actions de révision et de maintenance peuvent être omises des évaluations de PFD ;
- à la suite de chaque test complet, le système est restauré dans des conditions « comme neuves », de telle sorte que PFD_{avg} peut être évaluée sur l'intervalle de temps entre deux tests complets.

II.1.2.2. Notations

Les notations suivantes sont utilisées dans les Sections II.1.2 et II.1.3, et plusieurs d'entre elles sont décrites sur la Figure II.1.1.

*M*oo*N*	architecture du système (cf. Section II.1.2.1), avec $M \leq N$
λ	taux de défaillance de chacun des éléments du système
$A_e(t)$	disponibilité de chacun des éléments du système au temps t, c'est-à-dire la probabilité que l'élément soit capable d'accomplir la fonction de sécurité au temps t
$A(t)$	disponibilité du système au temps t, c'est-à-dire la probabilité que le système soit capable d'accomplir la fonction de sécurité au temps t
$U(t)$	indisponibilité du système au temps t, i.e. $U(t) = 1 - A(t)$
t_i	instant d'exécution du $i^{ème}$ test de révision (qui peut être partiel ou complet), avec la condition initiale $t_0 = 0$ qui est assimilée à l'exécution du dernier test complet
T_i	intervalle de temps entre le $(i-1)^{ème}$ et le $i^{ème}$ test de révision, i.e. $T_i = t_i - t_{i-1}$

E efficacité des tests partiels, c'est-à-dire qu'une proportion égale à E du taux de défaillance de chacun des éléments du système correspond à des défaillances qui sont détectées lors de n'importe quel test partiel

n nombre total de tests dans un intervalle de temps entre deux tests complets, c'est-à-dire qu'il y a $(n-1)$ tests partiels, plus le $n^{ème}$ test qui est complet

τ intervalle de temps entre deux tests complets, i.e. $\tau = t_n$

PFD_i probabilité moyenne que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité moyenne) dans l'intervalle de temps entre le $(i-1)^{ème}$ et le $i^{ème}$ test de révision ($[t_{i-1} ; t_i]$)

PFD_{avg} probabilité moyenne que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité moyenne) dans l'intervalle de temps entre deux tests complets ($[0 ; t_n]$)

PFD_{max} probabilité maximale que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité maximale) dans l'intervalle de temps entre deux tests complets ($[0 ; t_n]$), i.e. $max(U(t))$ avec la condition $t_0 \leq t \leq t_n$

Obs_i probabilité de détecter une défaillance lors du $i^{ème}$ test de révision de chaque élément du système

k_i nombre (équivalent) d'éléments du système dont une défaillance a été détectée lors du $i^{ème}$ test de révision

K nombre total (équivalent) d'éléments du système qui ont été révisés (avec ou sans détection de défaillance, et suivi ou non d'actions de maintenance) lors du $i^{ème}$ test de révision

Un système est alors défini par l'ensemble (M, N, λ), et une politique de tests peut être défini de façon équivalente par l'ensemble $(E, t_1, t_2, \ldots, t_n)$ ou l'ensemble $(E, T_1, T_2, \ldots, T_n)$.

II.1.2.3. Expressions générales

Pour chaque élément du système, une partie avec un taux de défaillance égal à $E \cdot \lambda$ est révisable par n'importe quel test de révision, qu'il soit partiel ou complet, et l'autre partie avec un taux de défaillance égal à $(1-E) \cdot \lambda$ n'est révisable que par des tests complets. Le diagramme de fiabilité correspondant est décrit sur la Figure II.1.2, et (cf. preuves en Annexe, Section VI.1.1) :

$$A_e(t) = e^{E \cdot \lambda \cdot t_{i-1}} \cdot e^{-\lambda \cdot t} \qquad \text{pour } t_{i-1} \leq t < t_i \qquad \text{[II.1.1]}$$

La disponibilité du système au temps t est alors (cf. preuves en Annexe, Section VI.1.2) :

$$A(t) = \sum_{x=M}^{N} \left[S(M,N,x) \cdot e^{x \cdot E \cdot \lambda \cdot t_{i-1}} \cdot e^{-x \cdot \lambda \cdot t} \right] \qquad \text{pour } t_{i-1} \leq t < t_i \qquad \text{[II.1.2]}$$

avec la somme suivante, indépendante du temps t, et dont certaines valeurs sont données dans le Tableau II.1.1 :

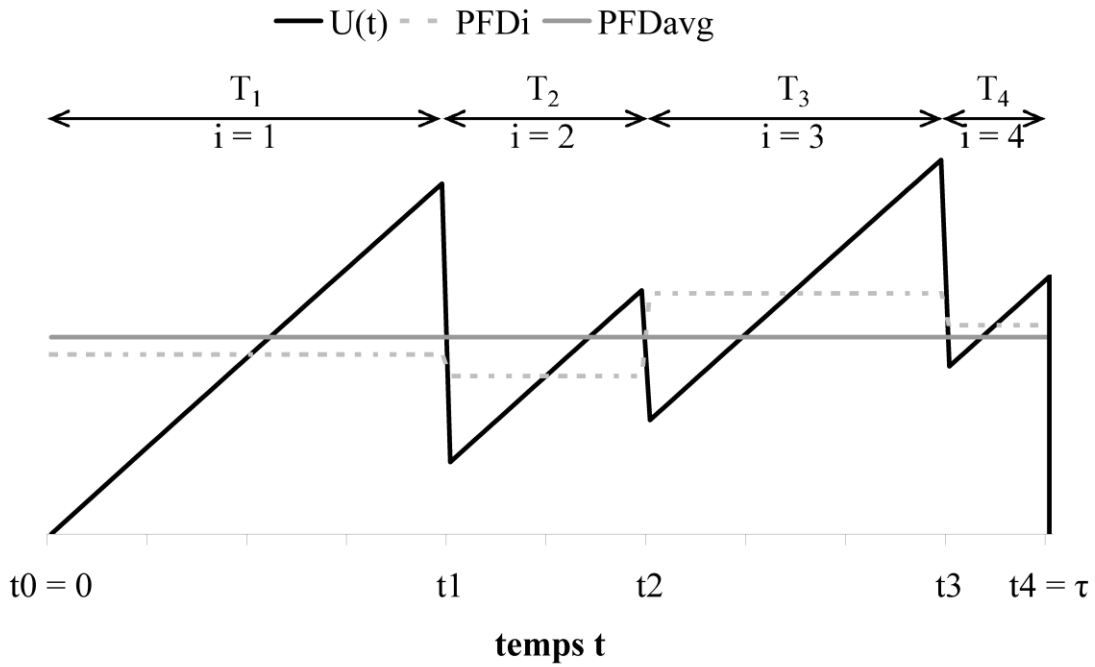

Figure II.1.1. Notations pour les probabilités de défaillance à la sollicitation (PFD), exemple avec *n = 4*

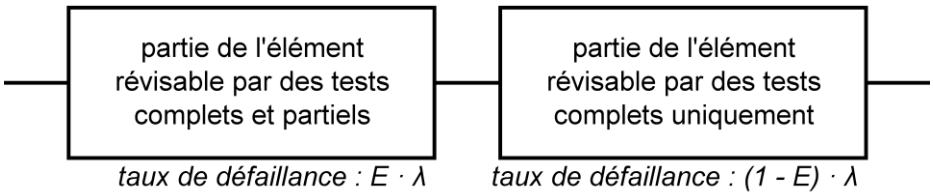

Figure II.1.2. Diagramme de fiabilité d'un élément soumis à des tests de révision complets et partiels

Tableau II.1.1. Valeurs des sommes *S(M, N, M)*, *S(M, N, M + 1)*, …, *S(M, N, N)*, pour différentes architectures *M*oo*N*

	N = 1	*N = 2*	*N = 3*	*N = 4*	*N = 5*
M = 1	*1*	*2, -1*	*3, -3, 1*	*4, -6, 4, 1*	*5, -10, 10, -5, 1*
M = 2		*1*	*3, -2*	*6, -8, 3*	*10, -20, 15, -4*
M = 3			*1*	*4, -3*	*10, -15, 6*
M = 4				*1*	*5, -4*
M = 5					*1*

$$S(M,N,x) = \sum_{k=M}^{x}\left[\binom{N}{x}\cdot\binom{x}{k}\cdot(-1)^{x-k} \right] \qquad \text{pour } x = M, \ldots, N \qquad \text{[II.1.3]}$$

Les probabilités moyennes que le système ne soit pas capable d'accomplir la fonction de sécurité, dans l'intervalle de temps entre le $(i-1)^{\text{ème}}$ et le $i^{\text{ème}}$ test de révision, et dans l'intervalle de temps entre deux tests complets, sont donc (cf. preuves en Annexe, Sections VI.1.3 et VI.1.4) :

$$PFD_i = 1 - \sum_{x=M}^{N}\left[S(M,N,x)\cdot e^{-x\cdot(1-E)\cdot\lambda\cdot t_{i-1}}\cdot\frac{1-e^{-x\cdot\lambda\cdot T_i}}{x\cdot\lambda\cdot T_i} \right] \qquad \text{[II.1.4]}$$

$$PFD_{avg} = 1 - \sum_{x=M}^{N}\left[S(M,N,x)\cdot\sum_{i=1}^{n}\left[e^{-x\cdot(1-E)\cdot\lambda\cdot t_{i-1}}\cdot\frac{1-e^{-x\cdot\lambda\cdot T_i}}{x\cdot\lambda\cdot\tau} \right] \right] \qquad \text{[II.1.5]}$$

Lorsque le produit $\lambda \cdot \tau$ est relativement faible ($\lambda \cdot \tau < 10^{-2}$), les approximations suivantes peuvent être faites, en utilisant des développements de Taylor :

$$A_e(t) \approx 1 + E\cdot\lambda\cdot t_{i-1} - \lambda\cdot t \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[II.1.6]}$$

$$A(t) \approx 1 - \binom{N}{M-1}\cdot\lambda^{N-M+1}\cdot\left(t - E\cdot t_{i-1}\right)^{N-M+1} \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[II.1.7]}$$

$$PFD_i \approx \binom{N}{M-1}\cdot\frac{\lambda^{N-M+1}}{N-M+2}\cdot\frac{1}{T_i}\cdot\left(\left(t_i - E\cdot t_{i-1}\right)^{N-M+2} - \left(t_{i-1}\cdot(1-E)\right)^{N-M+2}\right) \qquad \text{[II.1.8]}$$

$$PFD_{avg} \approx \binom{N}{M-1}\cdot\frac{\lambda^{N-M+1}}{N-M+2}\cdot\frac{1}{\tau}\cdot\sum_{i=1}^{n}\left[\left(t_i - E\cdot t_{i-1}\right)^{N-M+2} - \left(t_{i-1}\cdot(1-E)\right)^{N-M+2} \right] \qquad \text{[II.1.9]}$$

II.1.2.4. Cas particulier sans test partiel

Sans test partiel, $n = 1$ et $t_1 = t_n = \tau$, et les Équations II.1.2, II.1.7, II.1.5, et II.1.9, deviennent respectivement :

$$A(t)^{(w)} = \sum_{x=M}^{N}\left[S(M,N,x)\cdot e^{-x\cdot\lambda\cdot t} \right] \qquad \text{pour } 0 \le t < \tau \qquad \text{[II.1.10]}$$

$$A(t)^{(w)} \approx 1 - \binom{N}{M-1}\cdot\left(\lambda\cdot t\right)^{N-M+1} \qquad \text{pour } 0 \le t < \tau \qquad \text{[II.1.11]}$$

$$PFD_{avg}{}^{(w)} = 1 - \sum_{x=M}^{N}\left[S(M,N,x)\cdot\frac{1-e^{-x\cdot\lambda\cdot\tau}}{x\cdot\lambda\cdot\tau} \right] \qquad \text{[II.1.12]}$$

$$PFD_{avg}{}^{(w)} \approx \binom{N}{M-1}\cdot\frac{\left(\lambda\cdot\tau\right)^{N-M+1}}{N-M+2} \qquad \text{[II.1.13]}$$

II.1.2.5. Cas particulier avec des tests partiels périodiques

Les tests partiels sont périodiques si $T_i = T_0$ pour $i = 1, \ldots, n$, c'est-à-dire que $t_i = i \cdot T_0$ pour $i = 1, \ldots, n$. Les Équations II.1.2, II.1.7, II.1.5, et II.1.9, deviennent alors respectivement :

$$A(t)^{(p)} = \sum_{x=M}^{N} \left[\; S(M,N,x) \cdot e^{x \cdot E \cdot \lambda \cdot (i-1) \cdot T_0} \cdot e^{-x \cdot \lambda \cdot t} \; \right] \qquad \text{pour } (i-1) \cdot T_0 \le t < i \cdot T_0 \qquad \text{[II.1.14]}$$

$$A(t)^{(p)} \approx 1 - \binom{N}{M-1} \cdot \lambda^{N-M+1} \cdot \left(t - E \cdot (i-1) \cdot T_0\right)^{N-M+1} \qquad \text{pour } (i-1) \cdot T_0 \le t < i \cdot T_0 \qquad \text{[II.1.15]}$$

$$PFD_{avg}{}^{(p)} = 1 - \sum_{x=M}^{N} \left[\; S(M,N,x) \cdot \frac{1 - e^{-x \cdot \lambda \cdot T_0}}{x \cdot \lambda \cdot T_0} \cdot \frac{1}{n} \cdot \sum_{i=1}^{n} \left[\; e^{-x \cdot (1-E) \cdot \lambda \cdot (i-1) \cdot T_0} \; \right] \right] \qquad \text{[II.1.16]}$$

$$PFD_{avg}{}^{(p)} \approx \binom{N}{M-1} \cdot \frac{(\lambda \cdot T_0)^{N-M+1}}{N-M+2} \cdot \frac{1}{n} \cdot \sum_{j=0}^{n-1} \left[\; (1 + j \cdot (1-E))^{N-M+2} - (j \cdot (1-E))^{N-M+2} \; \right] \qquad \text{[II.1.17]}$$

Dans le cas particulier où le système est sans redondance, c'est-à-dire avec $M = N = 1$, cette dernière équation conduit à une approximation que l'on trouve dans plusieurs références [ASu00b, MLu08b].

II.1.3. Cas d'Étude : Système de Mesure d'Oxygène

II.1.3.1. Description du cas d'étude

Le cas d'étude présenté ici est extrait d'une prestation effectuée par l'INERIS, et concerne un système de mesure de la concentration en oxygène dans l'air. Celui-ci fait partie d'un système d'inertage qui a pour objet de réduire la teneur en oxygène dans l'atmosphère d'une pièce (classiquement, un entrepôt), en y introduisant une quantité contrôlée d'azote. La concentration en oxygène doit alors être maintenue au dessous d'un seuil haut qui permet d'empêcher le départ d'incendie, et au dessus d'un seuil bas qui permet de maintenir l'atmosphère respirable. Afin de contrôler la concentration en oxygène, six capteurs-transmetteurs identiques sont utilisés. Parce que l'azote est répartie dans la pièce rapidement et de façon homogène, ces six capteurs-transmetteurs sont considérés comme redondants (ils mesurent les mêmes concentrations d'oxygène, aux mêmes valeurs). La fonction de sécurité ici étudiée consiste donc à détecter un seuil bas ou un seuil haut de concentration d'oxygène, selon une architecture établie à *2oo6*. (Cette fonction ne constitue ainsi qu'une partie de la fonction de sécurité du système d'inertage dans son ensemble, c'est-à-dire que pour vérifier le SIL maximal admissible pour la fonction de sécurité allouée au SIS, il convient également d'effectuer les évaluations correspondantes qui sont relatives aux autres éléments du système que sont les unités de traitement et les actionneurs.) Deux procédures de tests de révision des capteurs-transmetteurs sont alors recommandées par le fabricant du système :

- chaque année, des contrôles des résultats de mesure et, si nécessaire, suivis de réajustements, c'est-à-dire des tests qui peuvent être considérés comme complets ;
- occasionnellement, des inspections visuelles et quelques vérifications électroniques permises par des voyants lumineux, c'est-à-dire des tests partiels.

Pour des raisons de coûts, tous les six capteurs-transmetteurs sont révisés simultanément lors de chaque test de révision. La politique de tests de base consiste à exécuter un test complet tous les ans, et un test partiel tous les trois mois (tous les quatre tests partiels, ce dernier est confondu avec le test complet).

La première étape des analyses proposées dans la suite utilise le retour d'expérience des tests partiels et complets pour estimer les taux de défaillance des capteurs-transmetteurs, ainsi que l'efficacité des tests partiels. Ensuite, les PFD du système sont évaluées selon la politique de tests de base. Enfin, la répartition des tests partiels est optimisée afin de réduire PFD_{avg}.

II.1.3.2. Estimations paramétriques et évaluations des PFD

Lors du $i^{ème}$ test de révision de chaque capteur-transmetteur, la probabilité de détecter une défaillance est, d'après le diagramme de fiabilité décrit sur la Figure II.1.2 :

$$Obs_i \approx E \cdot \lambda \cdot T_i \qquad \text{pour } i = 1, \ldots, (n-1) \qquad \text{[II.1.18]}$$

et

$$Obs_i \approx E \cdot \lambda \cdot T_i + (1-E) \cdot \lambda \cdot \tau \qquad \text{pour } i = n \qquad \text{[II.1.19]}$$

De plus, puisqu'un nombre d'éléments k_i parmi K ont été détectés défaillants lors du $i^{ème}$ test de révision, un estimateur empirique de Obs_i est :

$$\hat{Obs}_i = \frac{k_i}{K} \qquad \text{pour } i = 1, \ldots, n \qquad \text{[II.1.20]}$$

Les estimateurs suivants, du taux de défaillance λ des capteurs-transmetteurs, et de l'efficacité E des tests partiels, peuvent alors être déduits des Équations II.1.18 à II.1.20 :

$$\hat{\lambda} = \frac{1}{K \cdot \tau} \cdot \sum_{i=1}^{n} k_i \qquad \text{[II.1.21]}$$

$$\hat{E} = \frac{\tau}{t_{n-1}} \cdot \frac{\sum_{i=1}^{n-1} k_i}{\sum_{i=1}^{n} k_i} \qquad \text{[II.1.22]}$$

Les résultats d'observations k_i sont, par nature, distribués selon une loi Binomiale. Des intervalles de confiance des estimations données par les Équations II.1.21 et II.1.22 peuvent alors être obtenus en utilisant des lois de Fisher [MRa02]. Des approches basées sur des « jugements d'experts » [PHo95] et des AMDEC [JBu09] ont également été proposées dans la littérature pour évaluer l'efficacité (ou la « couverture ») de tests partiels. Sur des bases qualitatives, des procédures ont aussi été développées dans ce but, pour être appliquées à des vannes de sécurité [MLu08b].

En considérant quatre installations, chacune d'elle exploitant six capteurs-transmetteurs de concentration d'oxygène, dont un retour d'expérience est disponible pour quatre années, le nombre

total équivalent de capteurs-transmetteurs révisés lors de chaque test de révision est $K = 4 \cdot 6 \cdot 4 = 96$. De plus, un nombre total de $k_1 = k_2 = k_3 = 16$ capteurs-transmetteurs ont été détectés défaillants lors des tests partiels, et $k_4 = 35$ capteurs-transmetteurs ont été détectés défaillants lors des tests complets. D'après les Équations II.1.21 et II.1.22, le taux de défaillance λ des capteurs-transmetteurs est estimé à $6.1 \cdot 10^{-5}$ par heure, et l'efficacité E des tests partiels est estimée à 0.42.

D'après l'Équation II.1.16, équivalente à l'Équation II.1.5 pour des tests partiels périodiques, PFD_{avg} est alors évaluée à $2.06 \cdot 10^{-3}$. PFD_{max} est quant à elle évaluée à $1.21 \cdot 10^{-2}$. Pour ce cas d'étude, les tests partiels ont permis de réduire PFD_{avg} par un facteur de 5, par rapport au résultat qui aurait été obtenu sans test partiel, par application de l'Équation II.1.12, et de réduire PFD_{max} par un facteur proche de 4. Les PFD du cas d'étude, selon la politique de tests partiels périodiques (politique de base), sont décrites sur la Figure II.1.3.

II.1.3.3. Optimisation de la répartition des tests partiels

Une optimisation de la politique de tests consiste à répartir le même nombre de tests partiels, dans le même intervalle de temps entre deux tests complets, afin de minimiser PFD_{avg}. Lorsque les coûts liés aux tests partiels sont indépendants des instants auxquels ils sont exécutés, cette approche permet alors d'améliorer des critères de sécurité, sans coût additionnel.

Les instants optimaux de tests partiels sont notés t_i^*, avec $i = 1, \ldots, (n-1)$, et les intervalles optimaux entre deux tests sont notés T_i^*, avec $T_i^* = t_i^* - t_{i-1}^*$. La politique de tests partiels optimisée est alors obtenue par la résolution du problème de minimisation suivant :

$$(t_1^*, t_2^*, \ldots, t_{n-1}^*) = arg\ min(PFD_{avg}) \quad \text{pour } t_1^* \leq t_2^* \leq \ldots \leq t_{n-1}^* \leq t_n \quad \text{[II.1.23]}$$

avec PFD_{avg}, définie par l'Équation II.1.5.

Pour ce cas d'étude, les instants optimaux de tests partiels, et les intervalles de temps correspondants, tels qu'obtenus par la résolution de l'Équation II.1.23, sont donnés dans le Tableau II.1.2 (lignes « tests partiels optimisés »). Avec cette politique de tests partiels optimisée, et d'après l'Équation II.1.5, PFD_{avg} est maintenant évaluée à $1.87 \cdot 10^{-3}$, et PFD_{max} est évaluée à $9.68 \cdot 10^{-3}$. Par rapport aux résultats obtenus pour la politique de tests partiels périodiques (politique de base) présentés dans la Section II.1.3.2, cette optimisation a ainsi permis de réduire PFD_{avg} d'environ 10%, et PFD_{max} de plus de 25%. Les PFD du cas d'étude, selon la politique de tests partiels optimisée, sont décrites sur la Figure II.1.4.

II.1.4. Conclusions Partielles et Perspectives

En introduisant des expressions générales pour l'évaluation des probabilités de défaillance à la sollicitation (PFD) de systèmes d'architecture *MooN* soumis à des tests de révision partiels et complets, ces travaux ont permis de montrer comment des approches probabilistes pouvaient apporter des éléments de réponse à la maîtrise des risques technologiques. La forme explicite des formules (exactes ou approximées) proposées les rendent relativement simple à exploiter, et permet d'estimer les performances du système et de la politique de tests de révision, et d'optimiser cette dernière assez directement. Il a en particulier été montré que la probabilité moyenne de défaillance à la sollicitation (PFD_{avg}) peut être réduite, simplement par une meilleure répartition (apériodique) du même nombre de tests partiels. D'intéressantes perspectives concernent alors l'amélioration de la sécurité à moindre coût.

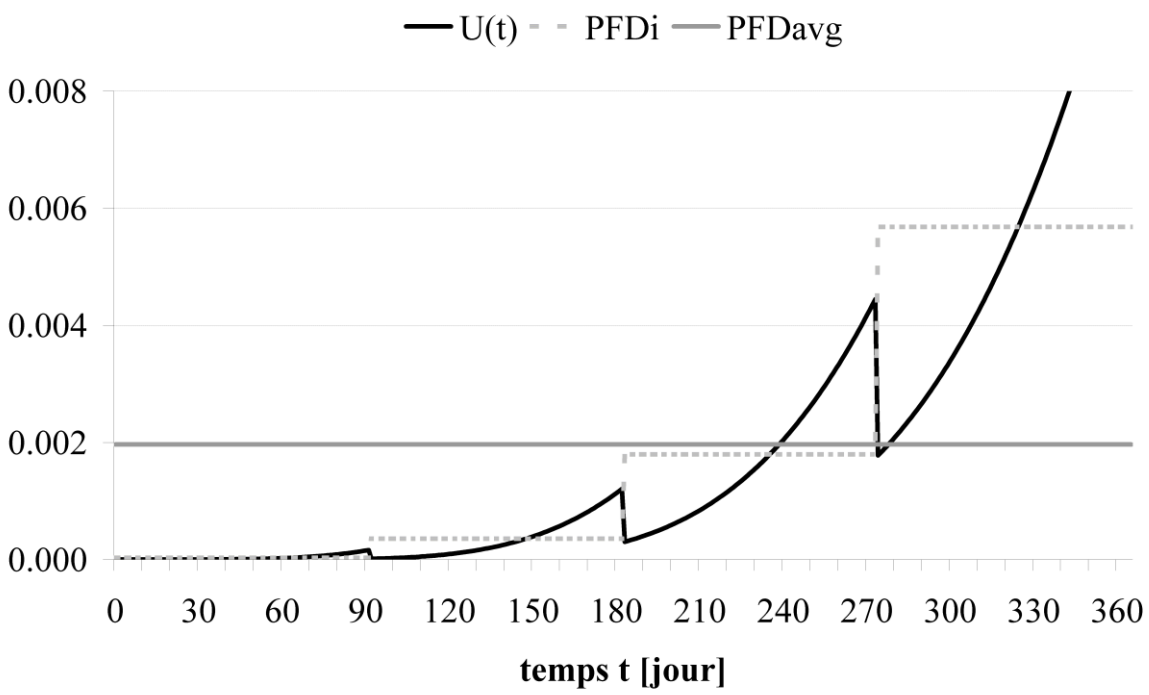

Figure II.1.3. Probabilités de défaillance à la sollicitation (PFD) du cas d'étude, selon la politique de tests partiels périodiques (politique de base)

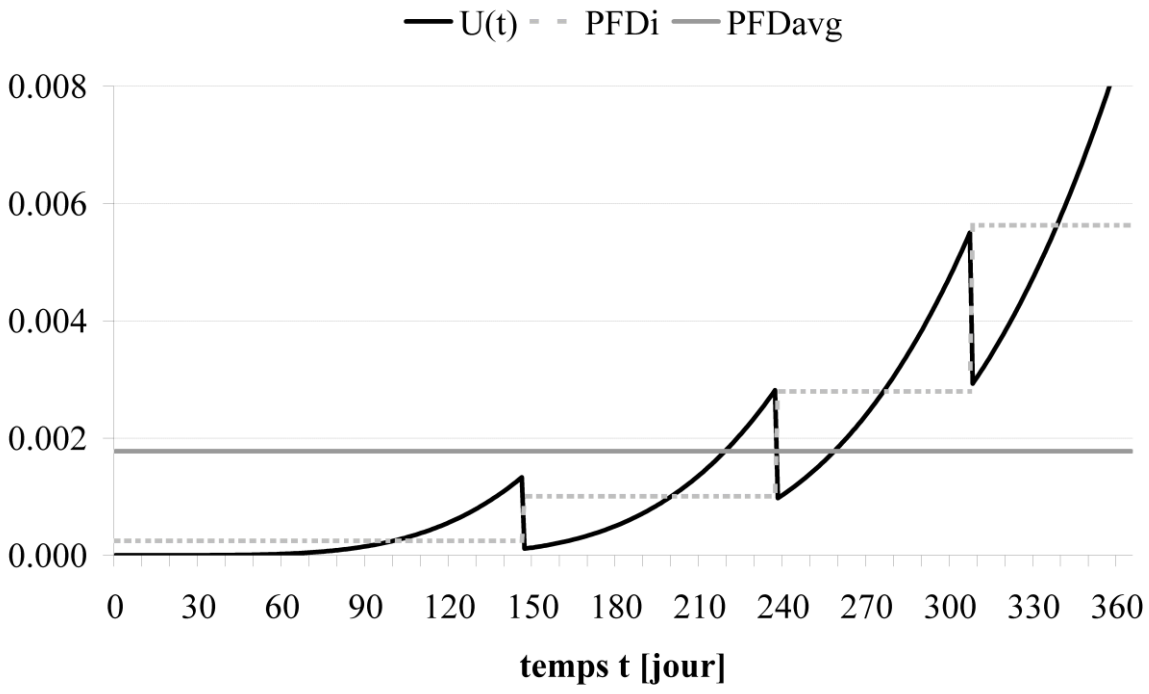

Figure II.1.4. Probabilités de défaillance à la sollicitation (PFD) du cas d'étude, selon la politique de tests partiels optimisée

Tableau II.1.2. Résultats des probabilités moyennes de défaillance à la sollicitation (PFD_{avg}) du cas d'étude, selon les politiques de tests partiels

politique de tests partiels	répartition des tests partiels		probabilité moyenne de défaillance à la sollicitation (PFD_{avg})
	instants de tests	intervalles de tests	
sans test partiel	$t_1 = 12.0$ mois	$T_1 = 12.0$ mois	$1.03 \cdot 10^{-2}$
tests partiels périodiques (politique de base)	$t_1 = 3.0$ mois $t_2 = 6.0$ mois $t_3 = 9.0$ mois $t_4 = 12.0$ mois	$T_1 = 3.0$ mois $T_2 = 3.0$ mois $T_3 = 3.0$ mois $T_4 = 3.0$ mois	$2.06 \cdot 10^{-3}$
tests partiels optimisés	$t_1^* = 4.8$ mois $t_2^* = 7.8$ mois $t_3^* = 10.1$ mois $t_4^* = 12.0$ mois	$T_1^* = 4.8$ mois $T_2^* = 3.0$ mois $T_3^* = 2.3$ mois $T_4^* = 1.9$ mois	$1.87 \cdot 10^{-3}$

Plusieurs des hypothèses présentées dans la Section II.1.2.1 sont aisément vérifiées lorsque des mesures sont prises afin de maintenir un état de sécurité au cours des actions de révision et de maintenance. Cependant, d'autres hypothèses pourraient être relâchées afin de fournir des outils de maîtrise des risques qui conviendraient à un plus large champ d'applications, par exemple à :

- des systèmes constitués d'éléments hétérogènes (éléments dont les taux de défaillance ne sont pas tous identiques) ;
- des systèmes sujets à des causes communes de défaillance (ce qui est particulièrement pertinent dans le cas d'étude de systèmes très redondants comme celui exposé dans la Section II.1.3) ;
- des systèmes d'architectures *M*oo*N* étendues (par exemple, des architectures *M*oo*N* imbriquées les unes dans les autres) ;
- des systèmes vieillissants (dont certains taux de défaillance ne sont pas constants) ;
- des politiques de tests avec des propriétés stochastiques, etc.

La plupart de ces cas peuvent être facilement résolus par des raisonnements similaires à ceux présentés dans la Section II.1.2.3, mais rendent souvent les expressions générales plus difficiles à manipuler. Parmi les autres développements envisageables, il conviendrait d'exprimer formellement les intervalles de confiance des estimations données par les Équations II.1.21 et II.1.22, ainsi que la solution du problème de minimisation de l'Équation II.1.23. Enfin, d'intéressantes perspectives concernent également l'inclusion de tests de révision asynchrones (en anglais, « *staggered tests* ») [MRa02, JRo06, YDu08a, YDu08b, YLa08, ATo09, JVa11] qui permettent aussi de réduire les PFD d'un système, souvent à moindre coût, en révisant ses éléments de façon échelonnée, ou selon des intervalles de temps différents.

II.2. ÉVALUATION DES TAUX DE DÉFAILLANCE EN FONCTION DES FACTEURS D'INFLUENCE

II.2.1. Taux de Défaillance et Facteurs d'Influence

Les évaluations quantitatives de la sûreté de fonctionnement (par exemple, fiabilité, disponibilité) d'un système nécessitent des modèles appropriés (par exemple, expressions générales, diagrammes de fiabilité, arbres de défaillance, chaînes de Markov, réseaux de Petri), ainsi que des données d'entrée. Parmi ces données, les taux de défaillance sont des paramètres incontournables. Le taux (instantané) de défaillance d'une entité au temps t est défini par la probabilité conditionnelle pour qu'une défaillance de l'entité se produise dans l'intervalle de temps $[t ; t + \Delta t]$, sachant que l'entité est restée opérante jusqu'au temps t, divisée par Δt, et lorsque Δt tend vers la valeur nulle. Le taux de défaillance peut alors être utilisé dans des modèles d'évaluation des probabilités de défaillance, par exemple ceux présentés dans la Section II.1.

La manière « idéale » d'obtenir une valeur de taux de défaillance est l'analyse du retour d'expérience [ALa96]. Cependant, par manque d'informations issues du retour d'exploitation, des valeurs « génériques » de taux de défaillance, fournies par des bases de données, sont couramment utilisées. Celles-ci résultent de l'expérience formalisée de certains secteurs d'activité, notamment des exploitations pétrolières offshore [ORE09, SIN10], du nucléaire [HPr98], et du militaire [RIA95, RIA97]. Les utilisateurs de ces bases font le postulat que les données ainsi fournies peuvent être transposées à leurs systèmes, et pour leurs applications, bien que les conditions techniques, opérationnelles, et environnementales, ne soient que rarement détaillées. Dans la suite, les *facteurs d'influence* sont définis par les agents internes ou externes à un système qui ont un effet sur sa fiabilité. Ces effets peuvent être positifs, en provoquant une réduction de l'intensité des défaillances, ou négatifs, en provoquant une augmentation de cette intensité. Les facteurs d'influence peuvent expliquer des différences souvent significatives entre les taux de défaillance de différents systèmes, comme le laisse supposer les écarts de valeurs observables entre les bases de données. L'utilisation de ces bases sans considération pour ces facteurs peut alors conduire à de fortes imprécisions dans les résultats d'évaluation des risques.

Pour répondre à ces problématiques, des modèles prédictifs « de stress » (ou « d'influence des contraintes » [IEC96]) pour taux de défaillance ont été développés, en particulier pour les composants électroniques. La première référence introduisant ce type de modèle est la MIL-HDBK-217, qui est apparue des les années soixante pour des applications militaires, et dont la version révisée de 1991 [USD91] est maintenant également connue et utilisé par dans l'industrie. Des taux de défaillance de composants électroniques y sont exprimés sous une forme analytique, qui dépend directement de certains paramètres, par exemple de diverses températures, de la tension et de l'intensité électrique. Une valeur de base correspond aux conditions de référence. Des coefficients y sont ensuite multipliés en fonction des facteurs d'influence (en anglais, cette partie est nommée « *part stress analysis* »). Le taux de défaillance d'un système est alors obtenu en additionnant les taux de défaillance de chacun de ses composants (en anglais, cette partie est nommée « *part count analysis* »). Depuis, plusieurs références similaires ont vu le jour, principalement pour le militaire [RIA06, UTE04], et les télécommunications [Tel01, UTE03, BT95]. De plus, la norme CEI 61709 [IEC96] présente des conditions de référence pour de tels modèles. La référence NSWC-98-LEI [NSW98] propose quant à elle des modèles prédictifs « de stress » pour quelques composants mécaniques (par exemple, vannes, ressorts, joints, engrenages). Les facteurs d'influence pris en compte sont alors nombreux : température, pression, propriétés des fluides et des matériaux,

charges, exigences de performances, etc. Cependant, le nombre de composants disponibles dans ce type de référence semble trop limité pour permettre des analyses complètes de systèmes relatifs à la sécurité, notamment en ce qui concerne les éléments mécaniques. De plus, les valeurs requises pour certains facteurs d'influence sont souvent difficiles à obtenir (par exemple, températures internes, taux de cycle, propriétés des matériaux), et les conditions de référence ne correspondent pas toujours à celles applicables dans les industries des procédés.

Sans connaissance a priori des relations physiques entre taux de défaillance et facteurs d'influence, des approches statistiques ont également été proposées [CCP99, BDe04]. Des données issues du retour d'expérience sont alors analysées afin d'observer des tendances en fonction des facteurs d'influence. Sur des bases statistiques, un modèle de Cox [DCo72], combiné à une loi de Weibull, (en anglais, « *weibull proportional-hazards models* » [EEl90, MNe94]), a été introduit pour modéliser des taux de défaillance à la fois en fonction du temps et des facteurs d'influence [BLa06, FBrIP]. Pour le même sujet, l'utilisation des réseaux de neurones a aussi été envisagée [BLa07]. Cependant, les modèles entièrement statistiques nécessitent une grande quantité d'informations pour obtenir des résultats exploitables. Face à cela, un moyen de combiner des données statistiques avec des « jugements d'experts » consiste, par exemple, en l'utilisation de réseaux bayésiens [HLa07].

De façon plus globale, plusieurs travaux ont été développés afin de prendre en compte des facteurs humains et organisationnels dans les évaluations probabilistes des risques (EPR) [KDa94, RRo98, KØi01a, TAv06]. Cinq étapes représentatives de ce type d'approches peuvent alors être identifiées [RRo98] :

1. préparation des analyses, définition du champ d'étude et des objectifs ;
2. collecte des documents appropriés et des données ;
3. analyse qualitative, afin de définir le modèle général, sélectionner les facteurs d'influence, et établir les états actuels des facteurs ;
4. analyse quantitative, afin d'évaluer les effets de chaque facteur, et d'évaluer les résultats sur la base du modèle ;
5. vérification et documentation, formalisation des résultats.

Plusieurs outils ont alors été proposés pour l'étape qualitative, en particulier pour la définition du modèle et la sélection des facteurs d'influence, par exemple : « arbre conceptuel » [RRo98] ; « modèle organisationnel » [KØi01a] ; et « diagramme d'influence du risque » [TAv06]. Afin d'établir les états actuels des facteurs d'influence, des « jugements d'experts » sont souvent utilisés, par exemple via : des questionnaires et audits [KDa94] ; une échelle de jugement allant de « A » (meilleure référence dans l'industrie) à F (pire pratique) [TAv06] ; et des indicateurs [KØi01a]. Ensuite, une analyse quantitative permet de formuler un résultat final (par exemple, niveau de risque, probabilité de défaillance à la sollicitation) selon les changements potentiels des états des facteurs d'influence. Pour cela, des procédures de jugements consistent à attribuer un poids à chaque facteur d'influence afin de nuancer leurs effets. Des « jugements d'experts » sont alors systématiquement utilisés, à l'exception d'une approche basée sur des indicateurs et un modèle de Cox [KØi01a]. En fonction du modèle défini, les influences des facteurs sont sommées ou, par exemple, des réseaux bayésiens sont utilisés [PTr08], modifiant alors des valeurs de base.

Une nouvelle méthodologie d'évaluation des taux de défaillance en fonction des facteurs d'influence est proposée dans cette Section II.2. Celle-ci a été spécialement développée pour des évaluations de sûreté de fonctionnement (qui incluent, par exemple, des évaluations de probabilités de défaillance à la sollicitation) de systèmes relatifs à la sécurité (en tant qu'éléments ou groupe d'éléments de systèmes instrumentés de sécurité), mais est assez générale pour être également

applicable à d'autres types de systèmes. Cette méthodologie cherche alors à répondre aux caractéristiques suivantes :

- être suffisamment globale pour être utilisable face à la plus grande variété de systèmes relatifs à la sécurité et de facteurs d'influence ;
- inclure une analyse quantitative pour prendre en compte le retour d'expérience lorsque celui-ci est disponible ;
- inclure une analyse qualitative pour compenser le manque éventuel d'informations issues du retour d'expérience grâce à l'utilisation de « jugements d'experts » organisés ;
- fournir des résultats justifiés, qui dépendent logiquement des facteurs d'influence (afin d'obtenir des résultats d'évaluations cohérents) ;
- apporter des perspectives en termes d'évaluation des risques, notamment pour permettre une maîtrise des risques plus efficace en agissant à la fois sur les systèmes relatifs à la sécurité et les facteurs d'influence.

Pour cela, la méthodologie proposée combine différents aspects des approches introduites précédemment : la forme générale du modèle est similaire à celle des modèles prédictifs « de stress » (suivant les termes anglais : « *part count* » et « *part stress analyses* ») ; une analyse quantitative permet d'intégrer des données issues du retour d'expérience pour définir des valeurs de base et des intervalles a priori de taux de défaillance ; et une analyse qualitative, inspirée des approches sur les facteurs humains et organisationnels, permet de prendre en compte les effets des facteurs d'influence. Cette méthodologie est constituée de sept étapes décrites dans la Section II.2.2, et est illustrée par un cas d'étude dans la Section II.2.3.

II.2.2. Méthodologie d'Évaluation des Taux de Défaillance en fonction des Facteurs d'Influence

II.2.2.1. Présentation générale

De la même façon que pour les modèles prédictifs « de stress », le système est ici divisé en plusieurs groupes principaux de composants, appelés dans la suite « éléments ». De plus, le taux de défaillance du système est obtenu par la somme des taux de défaillance de ces éléments (structure série [MRa02]). Si la décomposition du système en plusieurs éléments ne permet pas de vérifier cette propriété (structure parallèle ou « série-parallèle »), l'approche présentée peut être appliquée individuellement à chaque sous-ensemble du système qui répond à une structure série, et les taux de défaillance ainsi obtenus doivent ensuite être combinés selon les règles de la théorie de la fiabilité.

Avoir une idée a priori du taux de défaillance d'un système dans son ensemble est souvent plus réaliste que de disposer du détail des taux de défaillance des éléments qui le composent. Le taux de défaillance de base de chaque élément est donc ici exprimé en pourcentage du taux de défaillance de base du système. Les effets des facteurs d'influences sont ensuite intégrés par des coefficients multiplicateurs. Chaque coefficient est associé à un unique facteur, et vice-versa. Si un élément est concerné par l'influence d'un facteur, son taux de défaillance de base est alors multiplié par le coefficient correspondant. De plus, la valeur de chacun de ces coefficients est définie d'après l'état du facteur d'influence auquel il est associé :

- si le facteur d'influence est jugé comme étant dans un état moyen pour la fiabilité, alors le coefficient d'influence associé est égal à *1* ;

- si le facteur d'influence est jugé comme étant dans un état plus souhaitable (respectivement, moins souhaitable) pour la fiabilité que les conditions moyennes, alors le coefficient d'influence associé est inférieur à *1* (respectivement, supérieur à *1*).

Ces propriétés sont résumées par les expressions suivantes (cf. nomenclature donnée dans le Tableau II.2.1) :

$$\lambda_s = \sum_{i=1}^{N} \lambda_i = \sum_{i=1}^{N} \left[\lambda_{i,base} \cdot \prod_{j \in J_i} C_j^* \right] \qquad \text{[II.2.1]}$$

et

$$\lambda_{i,base} = c_i \cdot \lambda_{s,base} \text{ avec } \sum_{i=1}^{N} c_i = 1 \qquad \text{[II.2.2]}$$

avec λ_s et λ_i, respectivement les taux de défaillance du système et des éléments *i* de celui-ci, prenant en compte les états actuels des facteurs d'influence ; $\lambda_{s,base}$ et $\lambda_{i,base}$, respectivement les taux de défaillance de base du système et des éléments *i* de celui-ci ; c_i, la contribution de l'élément *i* dans le taux de défaillance de base du système, avec $i = 1, \ldots, N$; *N*, le nombre d'éléments identifiés qui composent le système ; C_j^*, le coefficient d'influence associé au facteur d'influence *j*, prenant en compte l'état actuel de ce dernier ; et J_i, l'ensemble des indices de facteurs d'influence qui ont un effet sur l'élément *i*.

Afin d'obtenir des résultats qui concordent avec une échelle présupposée de taux de défaillance, un intervalle a priori, noté $[\lambda_{s,min} ; \lambda_{s,max}]$, est défini. L'idée fondamentale de la méthodologie présentée ci-après consiste alors à utiliser certains critères pour fixer le taux de défaillance du système à l'intérieur de cet intervalle, en fonction des facteurs d'influence. Le modèle général est fondé sur les principes suivants, représentés sur la Figure II.2.1 :

- le taux de défaillance de base du système ($\lambda_{s,base}$) est atteint lorsque l'ensemble des facteurs d'influence sont, globalement, dans des états moyens ;
- la borne inférieure (respectivement, la borne supérieure) de l'intervalle a priori du taux de défaillance du système ($\lambda_{s,min}$, respectivement $\lambda_{s,max}$) est atteinte lorsque l'ensemble des facteurs d'influence sont, globalement, à une proportion égale à Ψ (le paramètre de sensibilité du modèle) des états les plus souhaitables (respectivement, les moins souhaitables) pour la fiabilité.

Sur la base de ces principes fondamentaux, et du modèle exprimé par les Équations II.2.1 et II.2.2, la méthodologie en sept étapes présentée dans les sections suivantes a pour objet de définir l'ensemble des paramètres requis par ce modèle, en particulier les coefficients d'influence C_j^*, par une exploitation « au mieux » des informations issues d'analyses quantitatives et qualitatives.

II.2.2.2. Méthodologie en sept étapes

II.2.2.2.1. Étape 1 : analyse fonctionnelle et données d'entrée

En premiers lieux, il convient de délimiter le champ d'étude : quel est le système considéré (par exemple, capteur-transmetteur, système de capteurs-transmetteurs, système instrumenté de sécurité dans son ensemble) ; quelle est la fonction étudiée de celui-ci ; et quelle est le taux de défaillance à évaluer (par exemple, taux des défaillances « dangereuses », exprimé « par heure » ou « par sollicitation »).

Tableau II.2.1. Nomenclature

paramètre	description
λ_s	taux de défaillance du système, prenant en compte les facteurs d'influence
$\lambda_{s,base}$	taux de défaillance de base du système
$\lambda_{s,min}$	borne inférieure de l'intervalle a priori du taux de défaillance du système
$\lambda_{s,max}$	borne supérieure de l'intervalle a priori du taux de défaillance du système
λ_i	taux de défaillance de l'élément *i* du système, prenant en compte les facteurs d'influence
$\lambda_{i,base}$	taux de défaillance de base de l'élément *i* du système
c_i	contribution de l'élément *i* dans le taux de défaillance de base du système
N	nombre d'éléments qui composent le système
Ψ	paramètre de sensibilité du modèle
I_j	indicateur du facteur d'influence *j*
$I_{j,inf}$	valeur inférieure de l'indicateur du facteur d'influence *j*
$I_{j,sup}$	valeur supérieure de l'indicateur du facteur d'influence *j*
$I_{j,moy}$	valeur observable moyenne de l'indicateur du facteur d'influence *j*
$I_{j,best}$	valeur observable la plus souhaitable de l'indicateur du facteur d'influence *j*
$I_{j,worst}$	valeur observable la moins souhaitable de l'indicateur du facteur d'influence *j*
$g_j(I_j)$	fonction d'indication pour l'indicateur du facteur d'influence *j*
F	matrice d'influence de dimension $N \cdot M$
M	nombre total de facteurs d'influence
J_i	ensemble des indices des facteurs d'influence qui ont un effet sur l'élément *i*
W_j	poids du facteur d'influence *j*
w_j	poids normalisé du facteur d'influence *j*
$C_j(I_j)$	fonction d'influence pour le facteur d'influence *j*

C^{+}_{ref}	coefficient d'influence de référence pour les conditions les plus souhaitables
C^{-}_{ref}	coefficient d'influence de référence pour les conditions les moins souhaitables
C_j^{*}	coefficient d'influence associé au facteur d'influence *j*

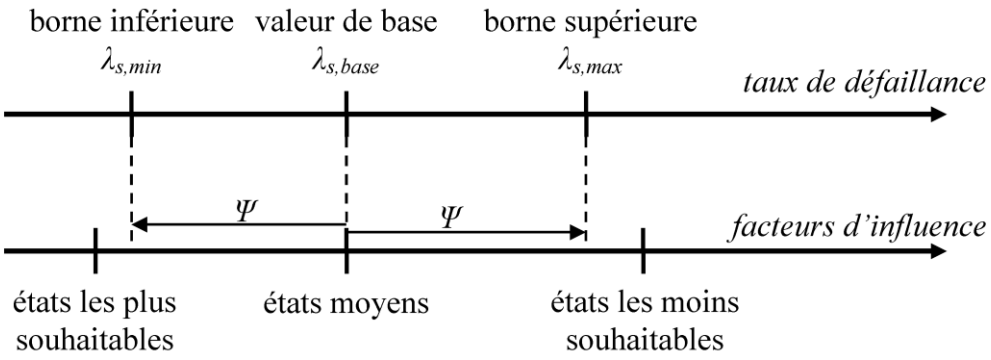

Figure II.2.1. Principe fondamental du model d'évaluation des taux de défaillance en fonction des facteurs d'influence

En exploitant d'éventuels retours d'expérience disponibles, des bases de données et, si nécessaire, des « jugements d'experts », le taux de défaillance de base du système ($\lambda_{s,base}$) doit être défini. Sa valeur doit refléter autant que possible les conditions moyennes, pour la fiabilité, dans lesquels le système peut se trouver. De plus, cette valeur est encadrée par un intervalle ($[\lambda_{s,min} ; \lambda_{s,max}]$), qui correspond aux taux de défaillance extrêmes envisageables pour ce système, d'après les états des facteurs d'influence considérés comme les moins et les plus souhaitables pour la fiabilité.

Une analyse des modes de défaillance, de leurs effets, et de leurs criticités (AMDEC) est recommandée afin d'identifier les éléments (groupes de composants) du système qui sont susceptibles d'être concernés par différents facteurs d'influence. Sur la base de cette AMDEC et, si possible, des données de fiabilité, la contribution de chaque élément (c_i, avec $i = 1, ..., N$) dans le taux de défaillance de base du système doit être évaluée.

II.2.2.2.2. Étape 2 : définition du modèle et sélection des facteurs d'influence

Un diagramme d'influence de la fiabilité est proposé pour la définition du modèle et la sélection des facteurs d'influence. Quatre niveaux sont représentés de droite à gauche, tels qu'illustrés dans la Section II.2.3 à l'aide d'un exemple :

1. le premier niveau représente le système ;
2. le second niveau est constitué des éléments du système qui ont été identifiés à la première étape de la méthodologie (cf. Section II.2.2.2.1) ; chaque élément de ce niveau est connecté au « système » du niveau précédent ;
3. le troisième niveau représente les phases du cycle de vie du système ; lorsque l'une de ces phases est supposée avoir une influence non négligeable sur la fiabilité de l'un des éléments du précédent niveau, alors une flèche est tracée entre ceux-ci ;
4. le dernier niveau représente les facteurs d'influence retenus pour chacune des phases du cycle de vie du système qui ont un effet sur la fiabilité de celui-ci.

Sur la base d'une analyse bibliographique, et d'études de terrain effectuées dans le domaine des industries des procédés, une checklist de facteurs d'influence a été établie. Celle-ci est donnée dans le Tableau II.2.2 et a pour objectif d'aider à la sélection des facteurs d'influence pertinents selon les phases de vie du système. Des facteurs humains et organisationnels peuvent également être ajoutés à l'aide de checklists spécifiques qui ont été proposées dans la littérature [JKi03, TAve06]. Le choix des facteurs d'influence doit se faire selon certains critères :

- il est possible de mesurer ou d'évaluer les états des facteurs d'influence (par l'intermédiaire d'indicateurs, cf. Section II.2.2.2.3) ;
- les états mesurés ou évalués des facteurs d'influence doit permettre de différencier les systèmes étudiés ;
- les facteurs d'influence retenus sont suffisamment exhaustifs pour expliquer les différences significatives en termes de fiabilité.

Une matrice d'influence, notée F et de dimension $N \cdot M$, est définie par : $F_{i,j} = 1$ si l'élément i du système est concerné par l'influence du facteur j, et $F_{i,j} = 0$ sinon, avec $i = 1, ..., N$ et $j = 1, ..., M$; M étant le nombre total de facteurs d'influence retenus.

II.2.2.2.3. Étape 3 : sélection et graduation des indicateurs

Un indicateur est le moyen par lequel l'état d'un facteur d'influence est observé. Des critères de sélection de tels indicateurs ont été proposés dans la littérature [KØi01b], notamment en termes de :

Tableau II.2.2. Checklist pour la sélection des facteurs d'influence

catégorie	sous-catégorie	facteur d'influence
conception		type de système principe de fonctionnement dimensions (e.g. taille, poids, capacité) matériaux qualité des composants (e.g. exigences, contrôles) caractéristiques particulières (e.g. alimentation)
fabrication		fabricant procédé de fabrication (e.g. procédures, contrôles)
installation et mise en service		localisation (e.g. facilités d'accès) assemblage et activation (e.g. procédures, contrôles)
utilisation	EUC	type de l'équipement commandé (EUC) caractéristiques particulières
	sollicitation	type de charge (e.g. cyclique, aléatoire) fréquence de sollicitation charge de sollicitation / seuil de déclenchement
	environnement	contraintes mécaniques (e.g. vibrations, chocs) températures corrosion / humidité pollutions (e.g. poussières, impuretés, « gaz poisons ») autres stresses (e.g. électromagnétiques, climatiques)
	exigences	exigences de performance modes des défaillances prises en compte
maintenance		fréquence des actions de maintenance préventive qualité des actions de maintenance préventive qualité des actions de maintenance corrective

quantité de données ; sources disponibles ; relations avec les facteurs observés ; validité ; et répétabilité.

Pour le modèle proposé, un (et un seul) indicateur doit être défini pour chaque facteur d'influence retenu. De plus, ces indicateurs doivent être transcrits sur une échelle numérique. Pour des indicateurs qualitatifs (par exemple, matériaux, fabricant), une échelle allant de *0* pour « très peu souhaitable pour la fiabilité » à *5* pour « très souhaitable pour la fiabilité » peut, par exemple, être utilisée. Pour des indicateurs quantitatifs (par exemple, dimensions, fréquence de sollicitation, températures), les valeurs obtenues peuvent être directement utilisées si elles remplissent les précédents critères, autrement, une échelle peut-être définie de la même façon que pour les indicateurs qualitatifs.

En utilisant des rapports techniques, des données d'exploitation, des informations issues du retour d'expérience et du personnel clef, des mesures, des études spécifiques, etc., trois valeurs particulières doivent être définies pour chaque indicateur : une qui représente l'état moyen du facteur d'influence ; et deux qui représentent les valeurs extrêmes observables (pour les états du facteur d'influence les plus et les moins souhaitables pour la fiabilité). L'échelle complète de l'indicateur, noté I_j, du facteur d'influence *j*, est notée $[I_{j,inf} ; I_{j,sup}]$, et les trois valeurs particulières sont notées $I_{j,moy}$ pour la valeur observable moyenne, $I_{j,best}$ et $I_{j,worst}$ pour, respectivement, la valeur observable la plus et la moins souhaitable pour la fiabilité.

II.2.2.2.4. Étape 4 : pondération des facteurs d'influence

Un poids est attribué à chaque facteur d'influence retenu. Celui-ci représente l'effet potentiel relatif sur les taux de défaillance des éléments concernés, selon une modification qui impliquerait un changement de la valeur d'indicateur correspondant de la valeur la moins souhaitable à la valeur plus souhaitable.

Une pondération des facteurs d'influence allant, par exemple, de *1* à *5* ou de *1* à *10* est généralement appropriée. Des informations issues du retour d'expérience, des procédures de comparaisons par pairs et de hiérarchisation, des tests, et des « jugements d'experts », peuvent, par exemple, être utilisés pour définir ces poids. Le poids attribué au facteur d'influence *j* est noté W_j, et il est normalisé avec l'expression suivante :

$$w_j = \frac{\sum_{i=1}^{N} c_i \cdot F_{i,j} \cdot W_j}{\sum_{i=1}^{N}\sum_{k=1}^{M} c_i \cdot F_{i,k} \cdot W_k} \qquad \text{[II.2.3]}$$

II.2.2.2.5. Étape 5 : fonctions d'indication

Pour prendre en compte certaines sources incertitudes, notamment lorsque des « jugements d'experts » sont nécessaires, des fonctions d'indication sont utilisées afin de représenter les valeurs actuelles des indicateurs, non pas par des valeurs déterministes, mais par des variables aléatoires. En effet, les valeurs d'indicateurs sont rarement connues avec précision et sont, de plus, souvent sujettes à des variations au cours du cycle de vie du système (par exemple, charge de sollicitation, températures, humidité). Les fonctions d'indication sont donc définies par des densités de probabilité, et trois types de lois sont proposés afin de représenter les distributions des valeurs d'indicateurs :

- des lois Uniformes, lorsque les « jugements d'experts » constituent la principale source d'évaluation des valeurs d'indicateurs ;
- des lois Triangulaires, si les valeurs d'indicateurs sont déterministes (et néanmoins traduites sur une échelle numérique, en utilisant une densité de probabilité) ;
- des lois Normales, lorsque les valeurs d'indicateurs sont quantitatives et directement utilisées en l'état.

Des exemples de ces trois types de lois sont donnés dans la Section II.2.3 à l'aide d'un cas d'étude. La fonction d'indication du facteur d'influence *j* (utilisée pour représenter les valeurs d'indicateur I_j) est notée $g_j(I_j)$, et est définie sur l'intervalle des valeurs d'indicateurs $[I_{j,inf} ; I_{j,sup}]$.

II.2.2.2.6. Étape 6 : fonctions d'influence

Les fonctions d'influence, notées $C_j(I_j)$ avec $j = 1, ..., M$, ont pour objet d'exprimer les coefficients d'influence en fonction des valeurs d'indicateurs. Un exemple conceptuel de ce type de fonction est décrit sur la Figure II.2.2. Chacune de ces fonctions est définie à partir de trois valeurs particulières : une qui correspond à la valeur observable moyenne de l'indicateur associé, notée $C_j(I_{j,moy})$; et deux qui correspondent respectivement à la valeur observable la plus et la moins souhaitable de l'indicateur associé, notées respectivement $C_j(I_{j,best})$ et $C_j(I_{j,worst})$. Ces valeurs peuvent être, par exemple, obtenues par l'intermédiaire du calcul de deux coefficients d'influence de référence, notés C_{ref}^{+} et C_{ref}^{-} pour, respectivement, les conditions globales les plus et les moins souhaitables, et obtenus par la résolution des équations suivantes :

$$\lambda_{s,\max} = \lambda_{s,base} \cdot \sum_{i=1}^{N} \left[\; c_i \cdot \prod_{j \in J_i} \left(\Psi \cdot w_j \cdot C_{ref}^{-} \right) \; \right] \qquad \text{[II.2.4]}$$

$$\lambda_{s,\min} = \lambda_{s,base} \cdot \sum_{i=1}^{N} \left[\; c_i \cdot \prod_{j \in J_i} \left(\frac{C_{ref}^{+}}{\Psi \cdot w_j} \right) \; \right] \qquad \text{[II.2.5]}$$

puis, par les expressions suivantes :

$$C_j\left(I_{j,base}\right) = 1 \qquad \text{pour } j = 1, ..., M \qquad \text{[II.2.6]}$$

$$C_j\left(I_{j,worst}\right) = w_j \cdot C_{ref}^{-} \qquad \text{pour } j = 1, ..., M \qquad \text{[II.2.7]}$$

$$C_j\left(I_{j,best}\right) = \frac{1}{w_j} \cdot C_{ref}^{+} \qquad \text{pour } j = 1, ..., M \qquad \text{[II.2.8]}$$

Ces valeurs particulières prennent ainsi en compte les précédentes étapes de la méthodologie, et notamment les poids attribués aux facteurs d'influence (cf. Section II.2.2.2.4). Des relations linéaires sont ensuite considérées entre ces valeurs, telles que décrites sur la Figure II.2.2. De plus, ces fonctions sont extrapolées sur les intervalles complets des valeurs d'indicateurs $[I_{j,inf} ; I_{j,sup}]$.

II.2.2.2.7. Étape 7 : résultats finaux

Sachant les fonctions d'indication ($g_j(I_j)$), qui expriment les états actuels des facteurs d'influence, et les fonctions d'influence ($C_j(I_j)$), qui expriment les coefficients d'influence, toutes en fonction des valeurs d'indicateurs (I_j), les coefficients d'influence, notés C_j^{*}, sont alors calculés par l'expression suivante :

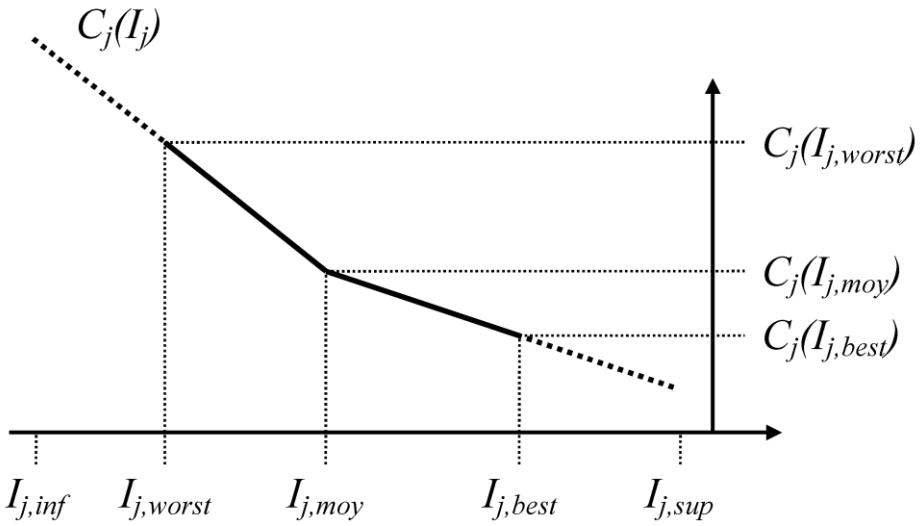

Figure II.2.2. Exemple conceptuel de fonction d'influence $C_j(I_j)$

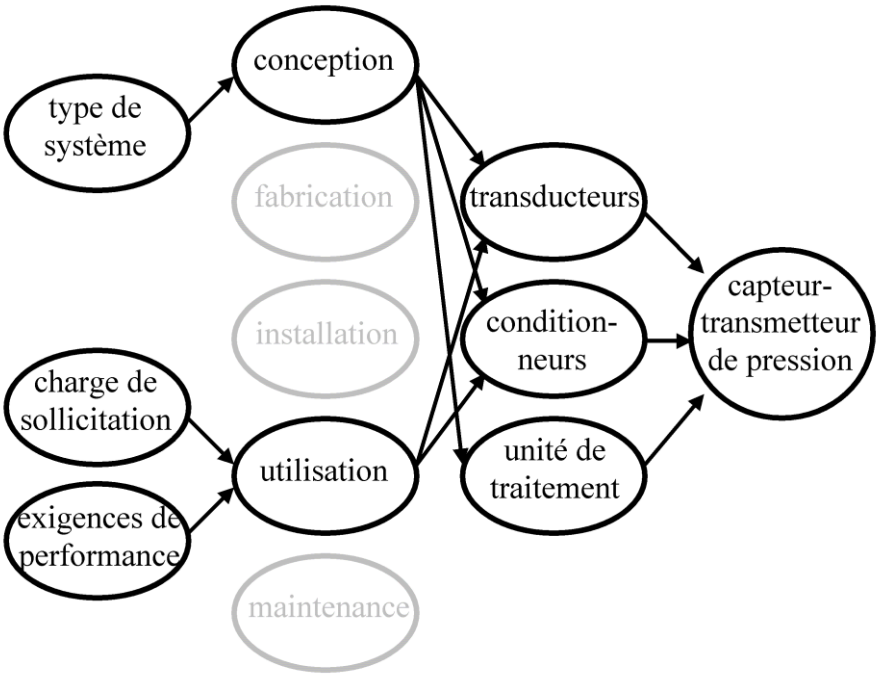

Figure II.2.3. Diagramme d'influence de la fiabilité appliqué au cas d'étude

$$C_j^* = \int_{I_{j,\inf}}^{I_{j,\sup}} C_j(I_j) \cdot g_j(I_j) \cdot dI_j \qquad \text{pour } j = 1, \ldots, M \qquad \text{[II.2.9]}$$

Enfin, le taux de défaillance final du système est obtenu par l'application des Équations II.2.1 et II.2.2, avec les données d'entrée définies lors de la première étape de la méthodologie (cf. Section II.2.2.2.1). L'utilisation de variables aléatoires pour les valeurs d'indicateurs (traduites dans l'Équation II.2.9 par les densités de probabilité définies par les fonctions d'indication $g_j(I_j)$) permet alors d'atténuer les effets potentiels de certaines hypothèses faites lors de la sixième étape de la méthodologie (cf. Section II.2.2.2.6, au sujet des définitions des fonctions d'influence).

II.2.3. Cas d'Étude : Capteurs-Transmetteurs de Pression

Afin d'illustrer la méthodologie développée, sept capteurs-transmetteurs de pression ont été considérés. Chaque capteur-transmetteur est décomposé en trois éléments : *transducteurs* (qui inclut notamment tous les « éléments sensibles » du système) ; *conditionneurs* (amplificateurs, filtres, etc.) ; et *unité de traitement* (en y incluant tous les ensembles liés aux traitements des données, et à la communication). Les contributions respectives de ces éléments dans le taux de défaillance de base de chaque capteur-transmetteur sont évaluées à *70*%, *5*%, et *25*%. Trois facteurs d'influence ont été retenus, qui correspondent aux phases de vie de conception et d'utilisation du système : le *type de système* (« gamme » du capteur-transmetteur) avec un poids attribué à *3* ; la *charge de sollicitation* (pression moyenne mesurée par le capteur-transmetteur) avec un poids attribué à *2* ; et les *exigences de performance* (écart limite entre la valeur du mesurande et la valeur mesurée avant de considérer le capteur-transmetteur comme défaillant) avec un poids attribué à *1*. Le diagramme d'influence de la fiabilité correspondant est décrit sur la Figure II.2.3. Les indicateurs respectifs de ces facteurs d'influence sont : la *catégorie de capteur-transmetteur*, classée selon trois classes nommées « *A* », « *B* », et « *C* » (indicateur qualitatif et déterministe) ; la *pression moyenne mesurée* [bars] par le capteur-transmetteur, qui est organisée en trois classes nommées « *faible pression* », « *pression moyenne* », et « *forte pression* », et dont les valeurs sont directement utilisées comme valeurs d'indicateur (indicateur quantitatif) ; et les *tolérances aux erreurs de mesure*, classées en deux classes nommées « *tolérances indulgentes* » et « *tolérances restrictives* » (indicateur qualitatif). Les Figures II.2.4 à II.2.6 décrivent les fonctions d'indication correspondantes, selon les recommandations de la cinquième étape de la méthodologie (cf. Section II.2.2.2.5). À noter, par exemple, qu'il a été considéré que plus la *pression moyenne mesurée* par le capteur-transmetteur est grande, et plus l'incertitude liée à cette valeur d'indicateur est grande. De plus, les valeurs d'indicateurs sont croissantes en fonction du « degré de souhaitabilité » (représenté par la clarté des courbes sur les Figures II.2.4 à II.2.6) pour les facteurs d'influence *type de système* et *exigences de performance* (cf. Figures II.2.4 et II.2.6), et décroissantes pour le facteur d'influence *charge de sollicitation* (cf. Figure II.2.5).

Les sept capteurs-transmetteurs de pression ont été ordonnés dans le Tableau II.2.3 selon la sévérité des facteurs d'influence, c'est-à-dire des meilleures aux pires conditions globales pour la fiabilité. En effet, pour chaque capteur-transmetteur *n*, le capteur-transmetteur *n + 1* possède au moins un facteur d'influence qui est dans un état moins souhaitable que pour le capteur-transmetteur précédent, et les autres facteurs d'influence sont dans les mêmes états. Une exception concerne les capteurs-transmetteurs *5* et *6* mais, parce que le facteur d'influence *charge de sollicitation* a un poids attribué qui est plus grand que le facteur d'influence *exigences de performance*, le capteur-transmetteur *6* est certainement dans des conditions globales moins souhaitables pour la fiabilité

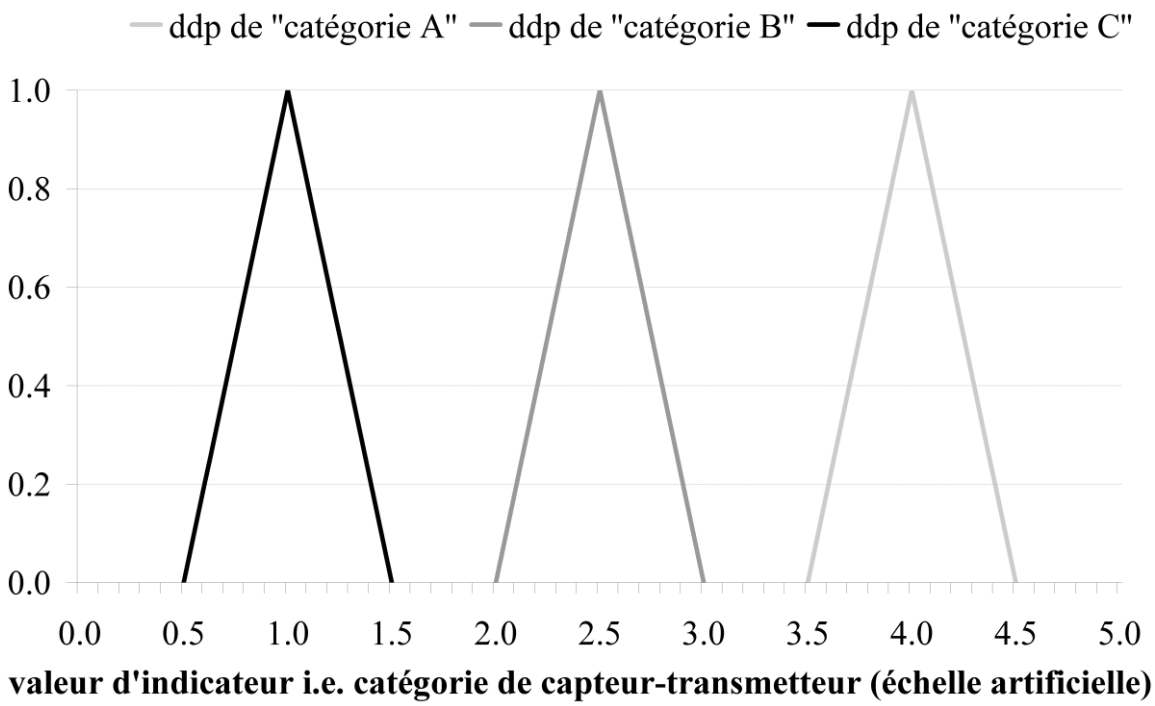

Figure II.2.4. Fonction d'indication (i.e. densité de probabilité (ddp)) pour le facteur d'influence *type de système*

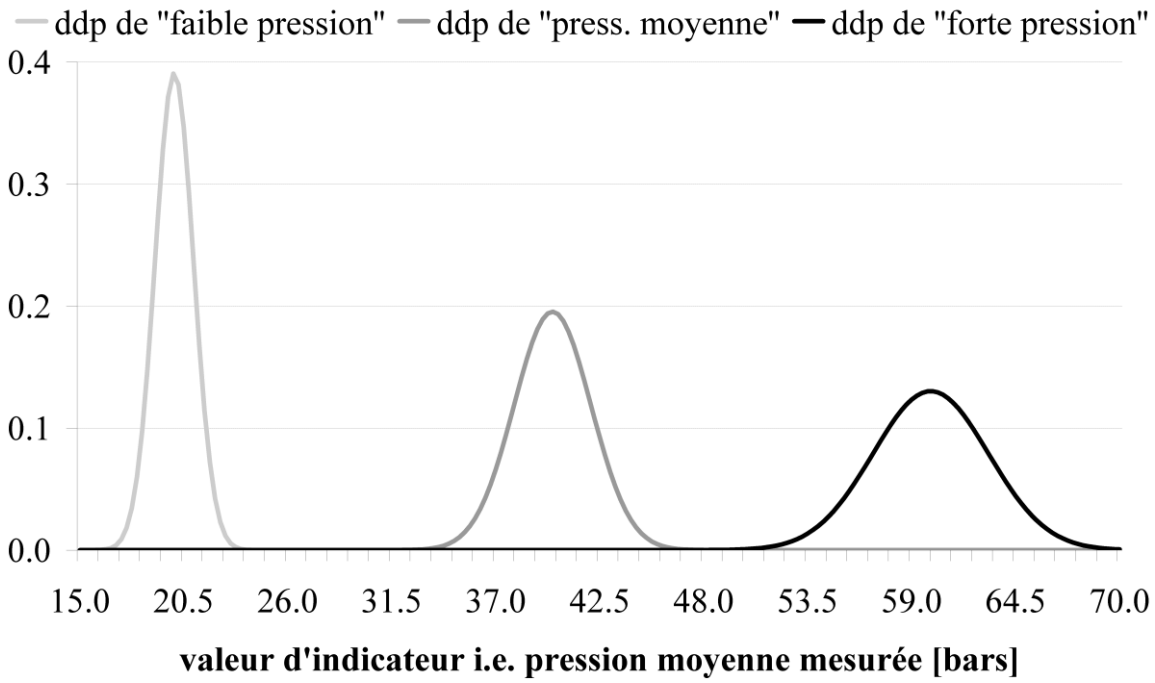

Figure II.2.5. Fonction d'indication (i.e. densité de probabilité (ddp)) pour le facteur d'influence *charge de sollicitation*

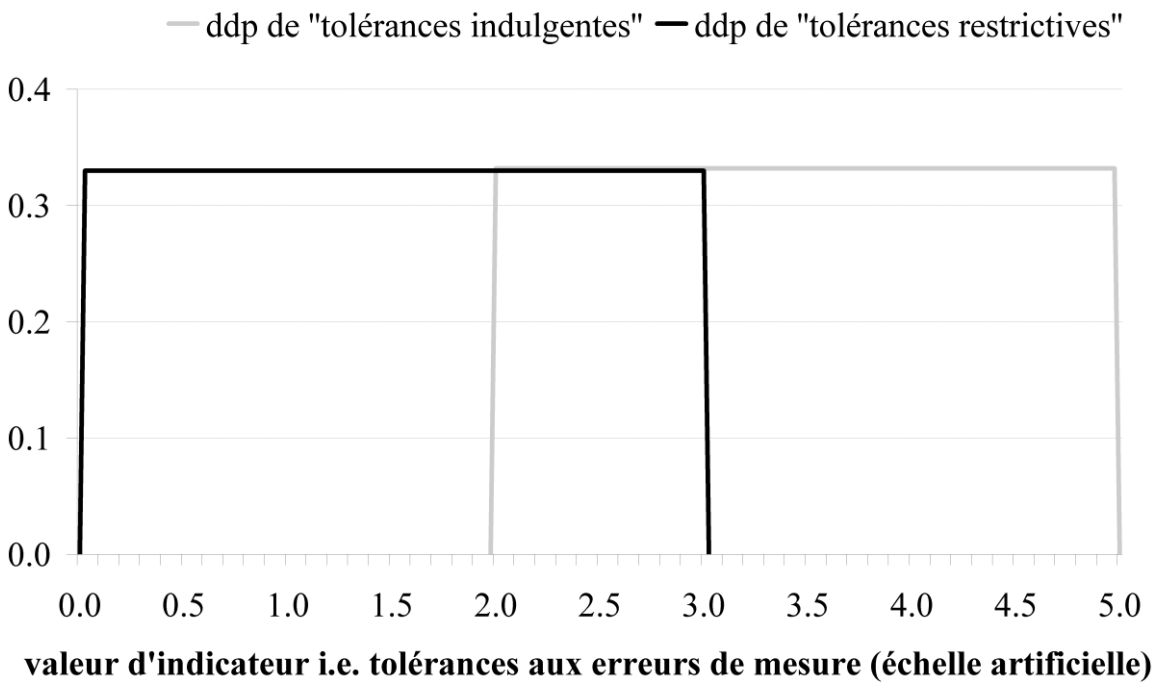

Figure II.2.6. Fonction d'indication (i.e. densité de probabilité (ddp)) pour le facteur d'influence *exigences de performance*

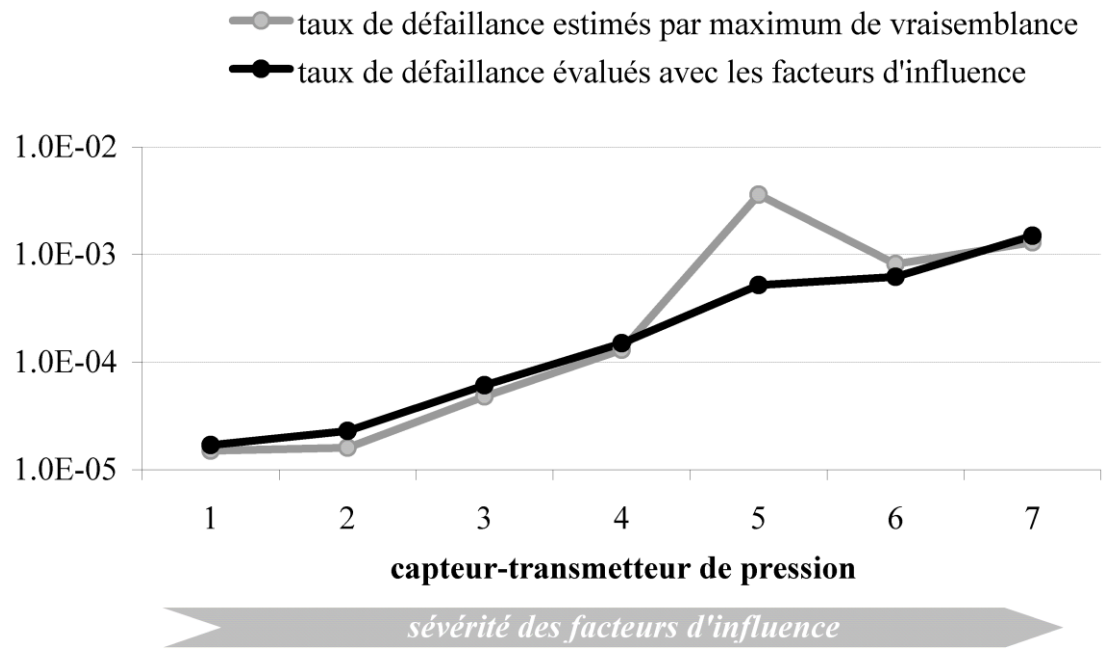

Figure II.2.7. Résultats des évaluations des taux de défaillance avec les facteurs d'influence, et des estimations par maximum de vraisemblance, pour les capteurs-transmetteurs de pression données dans le Tableau II.2.3

Tableau II.2.3. Les sept capteurs-transmetteurs de pression, ordonnés selon la sévérité des facteurs d'influence

indicateur (facteur d'influence)	capteur-transmetteur			
	1	*2*	*3*	*4*
catégorie (type de système)	*A*	*A*	*B*	*B*
pression moyenne mesurée (charge de sollicitation)	*faible*	*moyenne*	*moyenne*	*moyenne*
tolérance aux erreurs de mesure (exigences de performance)	*indulgentes*	*indulgentes*	*indulgentes*	*restrictives*
estimation par maximum de vraisemblance[a] [heure^{-1}]	$1.5 \cdot 10^{-5}$	$1.6 \cdot 10^{-5}$	$4.8 \cdot 10^{-5}$	$1.3 \cdot 10^{-4}$
évaluation avec les facteurs d'influence [heure^{-1}]	$1.7 \cdot 10^{-5}$	$2.3 \cdot 10^{-5}$	$6.1 \cdot 10^{-5}$	$1.5 \cdot 10^{-4}$

indicateur (facteur d'influence)	capteur-transmetteur		
	5	*6*	*7*
catégorie (type de système)	*C*	*C*	*C*
pression moyenne mesurée (charge de sollicitation)	*moyenne*	*forte*	*forte*
tolérance aux erreurs de mesure (exigences de performance)	*restrictives*	*indulgentes*	*restrictives*
estimation par maximum de vraisemblance[a] [heure^{-1}]	$3.6 \cdot 10^{-3}$	$8.2 \cdot 10^{-4}$	$1.3 \cdot 10^{-3}$
évaluation avec les facteurs d'influence [heure^{-1}]	$5.2 \cdot 10^{-4}$	$6.2 \cdot 10^{-4}$	$1.5 \cdot 10^{-3}$

[a]Les estimations par maximum de vraisemblance ont été obtenues d'après trois temps de bon fonctionnement avant défaillance, pour chaque capteur-transmetteur.

que le capteur-transmetteur *5*. Ce type d'arrangement n'est pas toujours faisable. Ici, les capteurs-transmetteurs ont été organisés de la sorte afin de faciliter la discussion sur le modèle proposé.

Peu de retour d'expérience est disponible, c'est-à-dire que seulement trois temps de bon fonctionnement avant défaillance ont été considérés pour chaque capteur-transmetteur. Des premières estimations des taux de défaillance ont alors été obtenues par la méthode du maximum de vraisemblance [MRa02]. Ces estimations sont données dans le Tableau II.2.3 et représentées sur la Figure II.2.7. On remarque alors que ces valeurs ainsi estimées sont incohérentes avec les états des facteurs d'influence. En effet, les capteurs-transmetteurs *1* et *2* se voient ainsi attribuer presque les mêmes taux de défaillance, bien que le second se trouve dans des conditions moins souhaitables pour la fiabilité (au regard de la *charge de sollicitation*). De plus, le capteur-transmetteur *5* se voit attribuer le plus grand taux de défaillance, bien qu'il ne soit pas celui qui se trouve dans les conditions les moins souhaitables pour la fiabilité. D'après l'arrangement donné dans le Tableau II.2.3, une allure « normale » de la courbe représentée sur la Figure II.2.7 devrait être strictement croissante. Ces incohérences peuvent être expliquées par le peu de données disponibles issues du retour d'expérience, qui ne permet alors pas d'obtenir ainsi des taux de défaillance avec un assez bon degré de confiance.

La méthodologie proposée a alors été suivie pour corriger ces premières estimations des taux de défaillance, afin de rendre les résultats plus cohérents d'après les états des facteurs d'influence. Le manque de données issues du retour d'expérience a donc pu être compensé par une analyse qualitative intégrant les facteurs d'influence. D'après les états des facteurs d'influence des sept capteurs-transmetteurs, les estimations par maximum de vraisemblance des capteurs-transmetteurs *3-4*, *1*, et *7*, sont utilisées comme données d'entrée pour la première étape de la méthodologie (cf. Section II.2.2.2.1), c'est-à-dire pour définir les taux de défaillance de base et extrêmes du système (respectivement, $\lambda_{s,base}$, $\lambda_{s,min}$, et $\lambda_{s,max}$). Les taux de défaillance obtenus par l'application de la méthodologie proposée sont donnés dans le Tableau II.2.3, et représentés sur la Figure II.2.7. On peut alors constater que les précédents problèmes de cohérence ont été corrigés par l'utilisation de la méthodologie proposée.

II.2.4. Conclusions Partielles et Perspectives

La méthodologie présentée combine une analyse quantitative pour intégrer les données disponibles issues du retour d'expérience, avec une analyse qualitative pour compenser les éventuels manques d'informations. Un fort retour d'expérience n'est donc pas nécessaire à l'application de cette démarche (contrairement aux approches exclusivement statistiques), et il n'est pas non plus indispensable de connaître précisément les états des facteurs d'influence et leurs effets sur la fiabilité (contrairement aux modèles prédictifs « de stress »).

L'évaluation des taux de défaillance en fonction des facteurs d'influence permet alors d'obtenir des résultats plus justifiés et cohérents. Parce que la méthodologie développée est suffisamment globale pour être utilisable face à la plus grande variété de systèmes relatifs à la sécurité et de facteurs d'influence, d'intéressantes perspectives concernent des applications liées à l'industrie des procédés. En effet, il est assez courant de trouver, dans ce secteur d'activité, des systèmes relatifs à la sécurité très hétérogènes (à la fois au regard des systèmes utilisés et des facteurs d'influence rencontrés), et où les retours d'expérience sont relativement rares. La méthodologie proposée permet alors de contribuer à une maîtrise des risques plus efficace, en agissant à la fois sur les systèmes relatifs à la sécurité et les facteurs d'influence. Une telle méthodologie prendrait alors tout son intérêt dans sa mise en application à grande échelle.

CHAPITRE III

MODÉLISATION ET ÉVALUATION DE CAPTEURS-TRANSMETTEURS À FONCTIONNALITÉS NUMÉRIQUES

Ce chapitre présente la modélisation et l'évaluation de « capteurs-transmetteurs intelligents » (CTI) en tant que systèmes à part entière. L'enjeu est de proposer une modélisation de ces systèmes qui prenne en compte l'ensemble de leurs interactions internes (matérielles et fonctionnelles), ainsi que leurs comportements mal connus en cas de défauts ou de défaillances, et ensuite de développer les analyses de fiabilité appropriées.

La première section de ce chapitre introduit une modélisation permettant de répondre à ces enjeux. La seconde section développe des analyses de fiabilité basées sur ce modèle. Enfin, la troisième section propose une extension du modèle initial pour effectuer plus efficacement des analyses d'incertitudes liées aux comportements du système.

Les publications réalisées en lien avec les travaux de ce chapitre sont présentées dans la Section VII.2.2.

SOMMAIRE DU CHAPITRE III

III.1. MODÉLISATION DE « CAPTEURS-TRANSMETTEURS INTELLIGENTS »

III.1.1. Modélisation de Systèmes Complexes

Un capteur-transmetteur intégrant des fonctionnalités numériques, plus communément qualifié de « capteur-transmetteur intelligent » (CTI), peut présenter deux niveaux de complexité :

- au niveau du système lorsque plusieurs interactions existent entre ses éléments matériels, entre ses éléments matériels et ses fonctions, et entre ses fonctions ;
- au niveau des composants du système lorsque certains de leurs comportements sont difficiles à définir (notamment en ce qui concerne les unités programmables et les logiciels).

Il est ainsi proposé d'examiner les modèles destinés aux systèmes complexes, selon des approches orientées *fonctions* ou *objets*.

Les approches orientées *fonctions* (ou les analyses fonctionnelles) permettent d'analyser un système selon les objectifs auxquels il doit répondre, et les fonctions qu'il doit réaliser. Ces approches sont par exemple utilisées en phase de conception afin de définir les exigences fonctionnelles du système, ou plus tard afin de comprendre son fonctionnement effectif [MLa99]. Elles incluent la *structured analysis and design technique* (SADT) [DRo77], telle que proposée par M. Robert *et al.* pour des CTI [MRo93] ; la *functional analysis system technique* (FAST), provenant des analyses de la valeur [MLa99] ; le *multilevel flow modelling* (MFM) [MLi94] ; et certains diagrammes de l'*unified modeling language* (UML) [OMG07b] ou du *system modeling language* (SysML) [OMG07a] (UML étendu pour les systèmes d'ingénierie), tels que les *use case diagrams*. La plupart de ces approches sont « semi-formelles » et différents modèles « corrects » peuvent être obtenus pour une même analyse [MLa99]. À l'origine « descriptives », elles présentent généralement certaines difficultés pour permettre, en l'état, des évaluations quantitatives. Une extension de la SADT, nommée safe-SADT [VBe08], a cependant été développée pour des analyses de sûreté de fonctionnement. Cette dernière peut, par exemple, être utilisée en phase de conception, lorsque le comportement du système peut être défini avec précision selon ses fonctions et ses éléments matériels.

Les approches orientées *objets* sont généralement plus formelles. Dans celles-ci, un système est organisé en une collection d'objets discrets [DLu95]. Elles sont par exemple utilisées pour décrire la structure statique ou dynamique du système selon ses éléments matériels (et logiciels) et leurs interactions (analyses structurelles). Une telle approche a par exemple été proposée par C.J. Garret *et al.* pour modéliser et analyser les comportements de systèmes numériques, par l'utilisation de la *dynamic flowgraph methodology* (DFM), afin d'identifier des évènements dangereux [CGa02]. D'autres exemples incluent les *arbres de défaillance*, et les *class diagrams* de l'UML (nommés *block definition diagrams* en SysML), similaires à ceux proposés par D. Luttenbacher *et al.* pour des CTI [DLu95]. Une fois le système défini selon ce formalisme, des outils de sûreté de fonctionnement peuvent être utilisés pour effectuer des analyses qualitatives [PDa09, PDa10], notamment des *analyses des modes de défaillance, de leurs effets, et de leurs criticités* (AMDEC), ainsi que des analyses quantitatives [DBo01]. Sur le même principe, le langage *AltaRica data-flow* a été spécialement développé pour effectuer des analyses de sûreté de fonctionnement [MBo06]. Les évaluations quantitatives sont alors généralement effectuées par l'intermédiaire de modèles de transitions entre états, le plus souvent par des réseaux de Petri. Parce que le système doit être strictement défini suivant le formalisme donné, ces approches sont, avant tout, appropriées lors des phases de conception.

En pratique, les approches orientées *fonctions* et *objets* ne constituent pas des concepts opposés, et ces deux approches peuvent être utilisées de manière complémentaire. Dans la suite, un formalisme de modélisation est présenté, qui décrit à la fois les aspects fonctionnels et matériels du système, selon une approche commune. Bien qu'un formalisme orienté *objets* soit préféré dans une optique de quantification, les analyses fonctionnelles sont néanmoins utiles pour définir les éléments appropriés du modèle. L'objectif de la modélisation proposée est de fournir un « modèle support » à des analyses de sûreté de fonctionnement. Ce modèle doit être en mesure de prendre en compte les interactions matérielles et fonctionnelles du système, ainsi que certains de ses comportements mal connus, comme il est souvent le cas lors d'études de CTI, notamment au-delà de la phase de conception.

III.1.2. Modélisation « 3-Step »

III.1.2.1. Modèle support basé sur les GTST-MLD

Le modèle développé ci-après est basé sur les *goal tree–success tree* (GTST), combinés aux *master logic diagrams* (MLD), tels que proposés par M. Modarres *et al.* [MMo93, MMo99]. Les GTST ont initialement été introduits dans les années 1980 pour des applications liées à la maîtrise des risques dans le domaine du nucléaire [RHu84, MRo85, MMo85b, MMo85a]. L'idée fondamentale est que les systèmes complexes (au sens des interactions entre les éléments du système, et à différents niveaux [HSi96, PCo85]) peuvent être mieux décrits par des structures hiérarchiques [MMo99]. Le système est alors décomposé selon ses « qualités » (objectifs et fonctions) par un *goal tree* (GT), et selon ses objets (parties) par un *success tree* (ST), telle que décrit sur la Figure III.1.1.

Le premier niveau du GT définit l'*objectif* du système, puis le second niveau est formé des *fonctions* qui doivent être réalisées pour atteindre cet objectif. Des niveaux supplémentaires peuvent être ajoutés pour préciser des *sous-fonctions*, jusqu'à ce que cette décomposition ne puisse continuer sans faire référence à des objets. Différents types de fonctions peuvent être distingués (par exemple, des fonctions principales et des fonctions de support) afin de faciliter les analyses de systèmes complexes. Ensuite, le ST décrit la structure du *système* selon des objets qui représentent les *parties* et *sous-parties* de celui-ci (hardware, software, et humains), requises pour la réalisation des fonctions du GT. Tout comme pour le GT, différents niveaux (par exemple, du système complet jusqu'à ses unités de base) et types d'objets (par exemple, éléments matériels principaux et éléments matériels de support) peuvent être distingués. De par ces décompositions, les relations entre les fonctions (fonctions et sous-fonctions) de niveaux voisins au sein du GT, ou entre les objets (parties et sous-parties) de niveaux voisins au sein d'un ST, sont directement représentées. De plus, ces relations peuvent être définies par des portes logiques (par exemple, de type « et » et « ou »). Par ailleurs, des relations peuvent aussi exister entre des fonctions de différents types au sein du GT, ou des objets de différents types au sein du ST, notamment lorsque que des éléments principaux et des éléments de support sont utilisés. La représentation de ces relations peut alors se faire au dépend de la clarté du modèle à cause de relations « croisées ». Enfin, et surtout, représenter de façon claire et concise les relations entre les fonctions du GT et les objets du ST (généralement entre sous-fonctions et sous-parties) est souvent encore plus problématique. En particulier pour les systèmes complexes, un objet du ST peut être utilisé pour réaliser plusieurs fonctions du GT, et vice-versa, plusieurs objets du ST peuvent être requis pour réaliser une seule fonction du GT.

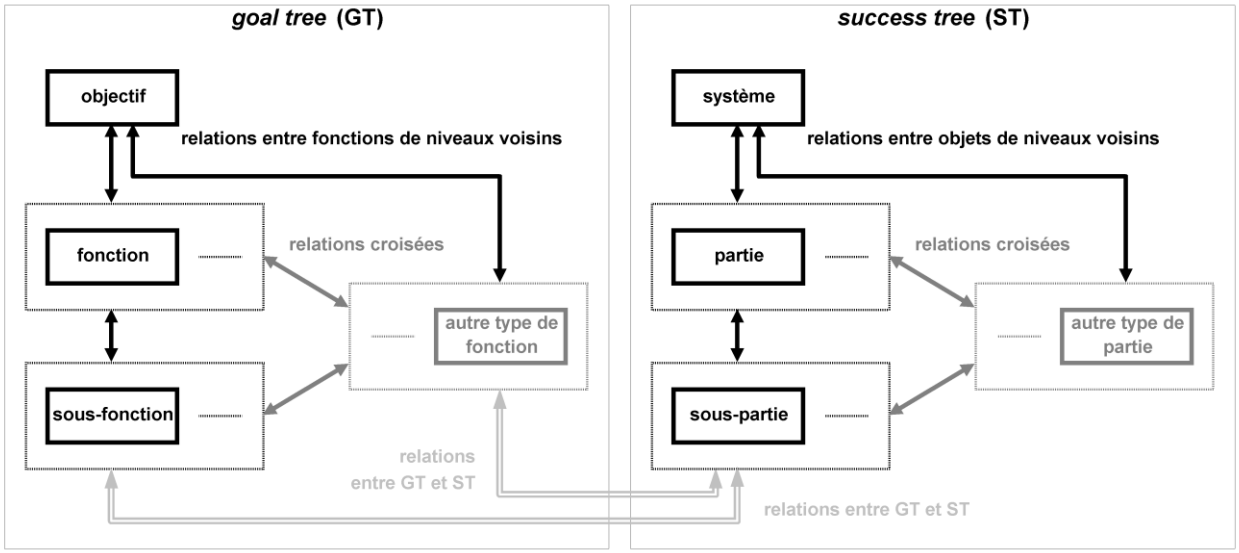

Figure III.1.1. Modèle conceptuel des GTST avec différents types de relations

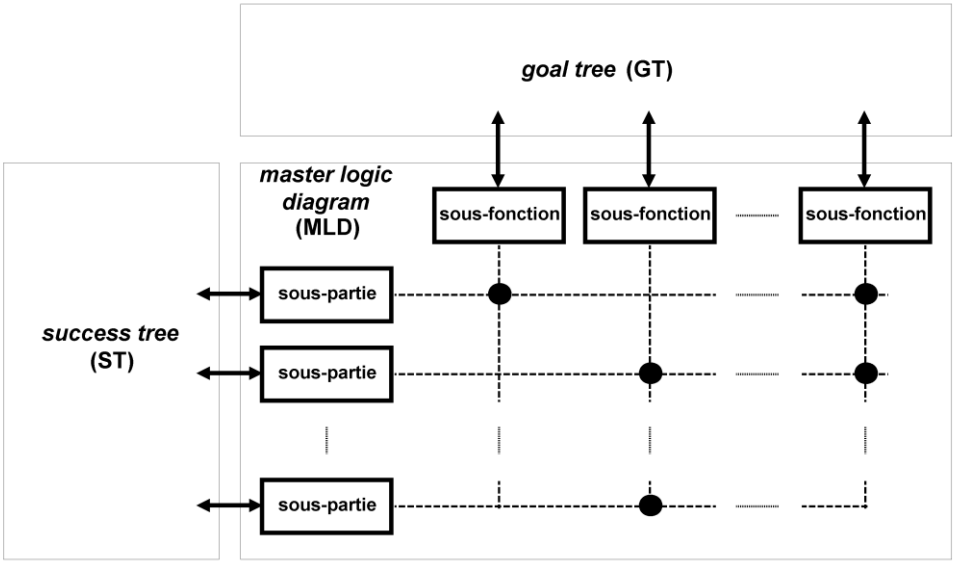

Figure III.1.2. Modèle conceptuel des GTST-MLD où les MLD sont utilisées pour représenter les relations entre les sous-fonctions du GT et les sous-parties du ST

Afin de représenter de façon compacte et transparente les relations entre les fonctions du GT et les objets du ST, ou entre différents types d'éléments au sein du GT ou du ST, des *master logic diagrams* (MLD) peuvent être utilisés [MMo99, IKi03, HMa00]. À titre d'exemple, un MLD est décrit sur la Figure III.1.2 pour représenter des relations entre les sous-fonctions identifiées dans le GT et les sous-parties du système identifiées dans le ST. Concrètement, un MLD prend la forme d'une matrice définie entre éléments donnés en aval (à gauche) et en amont (au dessus). Les relations entre ces éléments sont alors symbolisées par des cercles pleins en lieu des composantes de la matrice. Un tel cercle signifie que l'élément aval (à la gauche du point) est utilisé pour réaliser (face à une fonction), ou est une partie de (face à un objet), l'élément amont (au dessus du point). Dans le cas de relations entre des fonctions du GT et des objets du ST (comme sur la Figure III.1.2), les seconds sont donc les éléments aval et les premiers les éléments amont ; et respectivement pour des relations entre éléments principaux et éléments de support (fonctions ou objets). À noter que le terme « *master plan logic diagram* » (MPLD) a également été utilisé dans la littérature pour faire référence à ces mêmes matrices [MMo93, YHu96, HMa00]. En revanche, les MLD présentés ici ne doivent pas être confondus avec les *master logic diagrams* d'approches différentes, comme par exemple les MLD utilisés pour l'identification d'évènements dangereux ou initiateurs dans les analyses de risques [IPa03]. En français, nous utiliserons donc le terme plus explicite de « matrices de relations ».

L'approche combinée GTST-MLD fournit ainsi un moyen efficace de description des relations de causes à effets au sein de systèmes complexes [MMo99]. Par exemple, des modèles basés sur les GTST-MLD ont été utilisés pour analyser des comportements [YHu96, YHu99], ou pour identifier des défaillances [AJa98, HMa00], de certains complexes, et pour classer les parties d'un système en tant qu'éléments relatifs ou non à la sécurité [IKi03]. Dans le cadre des travaux présentés dans ce mémoire, un modèle support pour CTI est proposé, basé sur les GTST-MLD, et décrit sur la Figure III.1.3. En tant que tel, il convient de l'adapter selon les particularités propres aux systèmes considérés. La Figure III.1.3 inclut les éléments matériels ainsi que les fonctionnalités des CTI qui ont respectivement été présentées dans les Sections I.3.1.2 et I.3.1.3. Afin de se placer dans le cadre d'outils dédiés à la sûreté de fonctionnement, les termes français que nous utiliserons sont « arbres des fonctions » pour les GT, et « arbres des éléments matériels » pour les ST (cf. Sections suivantes). De plus, une représentation étendue des matrices de relations est proposée afin de représenter différents degrés de relations. Le modèle complet, présenté dans la suite, introduit également les défauts et les défaillances en tant que troisième composante, formant ainsi un modèle en trois parties (« 3-Step »). Cette dernière partie du modèle n'est pas représentée sur la Figure III.1.3, mais est décrite à l'aide d'un exemple sur la Figure III.1.4. Les trois parties de cette modélisation « 3-Step » (arbre des fonctions, arbre des éléments matériels, liste des défauts et des défaillances), ainsi que les matrices de relations, sont détaillées dans les sections suivantes.

III.1.2.2. Modèle « 3-Step » : fonctions, éléments matériels, défauts et défaillances

III.1.2.2.1. Arbre des fonctions

La première partie du modèle représente l'*aspect fonctionnel* du système. La définition des fonctions est le point d'entrée de toute analyse de sûreté de fonctionnement (cf. Section I.3.2.1), et notamment de fiabilité. En effet, la fiabilité d'un système se rapporte toujours à une (ou plusieurs) fonction, il s'agit de l'aptitude du système à réaliser une fonction requise (selon les exigences définies), dans des conditions données, et pendant un intervalle de temps donné [IEC90].

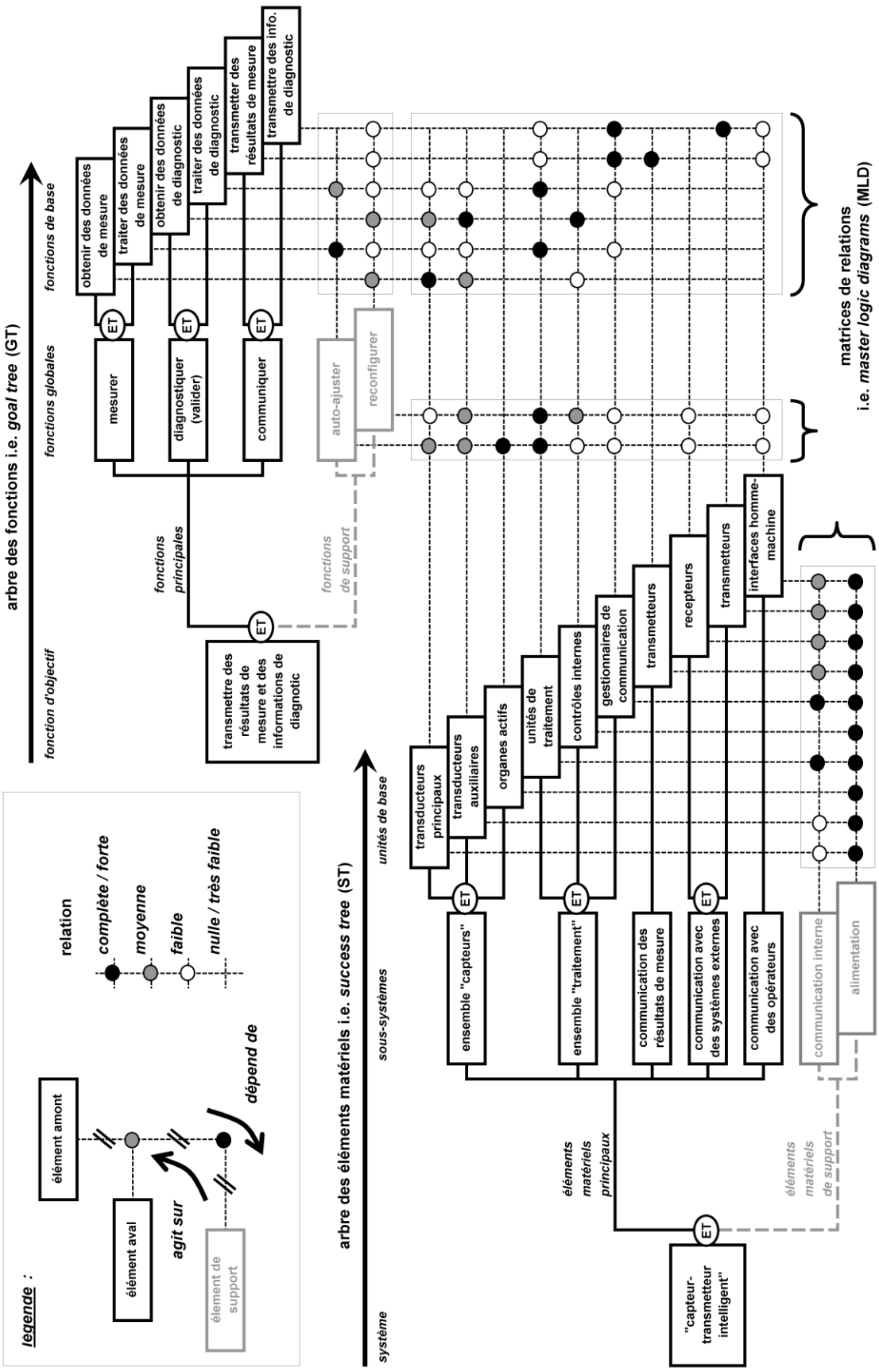

Figure III.1.3. Modèle support pour « capteur-transmetteur intelligent » (CTI)

La fonction du premier niveau (ou au sommet) de l'arbre des fonctions est alors la *fonction d'objectif*. Elle décrit sans ambiguïté l'objectif principal du système à analyser (une fonction est généralement exprimée par un verbe plus un ou plusieurs compléments). Classiquement, la fonction d'objectif est une fonction de sécurité, c'est-à-dire, une fonction utilisée pour prévenir l'occurrence d'un évènement dangereux, ou pour réduire les conséquences d'un tel évènement sur les personnes, l'environnement, ou les biens. Cette fonction doit être soigneusement définie d'après le champ d'étude. Par exemple, des conditions environnementales et des critères de performances peuvent être précisés.

La fonction d'objectif est divisée en sous-fonctions sur un second niveau plus détaillé. L'accomplissement des sous-fonctions, ensemble ou en combinaison, assure la réalisation de la fonction d'objectif. Ces relations peuvent être définies par des portes logiques. (Parce qu'un arbre des fonctions est orienté « réalisation » et non « défaillance », ces portes représentent le complément booléen des portes qui seraient utilisées dans l'arbre de défaillance correspondant.) Sur le même principe, les fonctions du second niveau peuvent à leur tour être décomposées en sous-fonctions sur un niveau suivant, et ainsi de suite. De cette façon, l'arbre des fonctions est créé en se demandant « comment » une fonction du niveau précédent est réalisée, jusqu'à ce que les fonctions du dernier niveau soient atteintes. En parcourant l'arbre dans l'autre sens, les fonctions du niveau courant doivent décrire « pourquoi » les fonctions du niveau suivant sont nécessaires. La construction de l'arbre peut alors prendre fin lorsque les fonctions ont suffisamment été décrites d'après le niveau de connaissance du système, et le champ d'étude. En accord avec le degré de détail utilisé pour les analyses, trois niveaux sont considérés dans la suite : *fonction d'objectif*, *fonctions globales*, et *fonctions de base*. De plus, uniquement des relations logiques de type « et » sont utilisées, c'est-à-dire que toutes les fonctions globales doivent être remplies pour réaliser la fonction d'objectif, et toutes les fonctions de base doivent être remplies pour réaliser les fonctions globales concernées (une approche moins restrictive sera ensuite introduite dans la Section III.3).

Différents types de fonctions peuvent être distingués [MRa96]. Dans l'approche proposée, deux types sont utilisés : *fonctions principales* et *fonctions de support*. Les fonctions globales et de base sont des fonctions principales car elles découlent directement de la décomposition de la fonction d'objectif. Les fonctions de support n'ont quant à elles pas d'objectif en soit en ce qui concerne l'utilisation du système, mais peuvent être requises par, ou agir sur, une ou plusieurs fonctions principales. Par exemple, une fonction de support peut fournir une ressource, une information, un contrôle, ou un environnement approprié, nécessaire à la réalisation d'une fonction principale. (Dans l'exemple de la Figure III.1.3, l'auto-ajustage est une fonction de support car elle définit des paramètres numériques qui sont utilisées lors du traitement des données de mesure et de diagnostic). Bien que certaines fonctions de support ne soient pas toujours faciles à identifier, elles peuvent se révéler très critiques pour la réalisation de la fonction d'objectif en ayant des effets sur plusieurs fonctions principales. Pour les CTI, les fonctionnalités présentées dans la Section I.3.1.3, et la Figure III.1.3, peuvent être utilisés afin d'éviter l'omission de certaines fonctions. Les relations entre les fonctions de support et la fonction d'objectif ne peuvent pas être directement représentées dans l'arbre par une branche parallèle à celles des fonctions principales, à cause des relations croisées. (Sur la Figure III.1.3, une ligne discontinue est ainsi utilisée pour relier les fonctions de support à la fonction d'objectif). Dans la suite, des matrices de relations sont donc utilisées pour représenter les relations entre les fonctions de support et les fonctions principales.

III.1.2.2.2. Arbre des éléments matériels

La seconde partie du modèle représente l'*aspect matériel* du système. Dans l'approche utilisée, l'objectif principal de cette partie est l'identification des éléments matériels, plus que la

représentation des relations physiques qui existent entre eux. Ainsi, le terme « arbre des éléments matériels » est préféré à celui de « arbre de succès » (qui serait une traduction plus juste de ST, et correspondrait au complément booléen des arbres de défaillance).

L'arbre des éléments matériels est formé des objets qui constituent le système, et qui sont requis à la réalisation des fonctions identifiées dans l'arbre des fonctions. Ces objets peuvent inclure de l'hardware, du software, et même des actions humaines ou des opérateurs humains, et sont qualifiés d'*éléments matériels* au sens large, par opposition à « qualité ». Ils sont alors identifiés à l'aide d'une décomposition du système en ses parties, puis chacune de ces parties en sous-parties, et ainsi de suite, créant ainsi un arbre des éléments matériels. En commençant par l'élément matériel du premier niveau (ou au sommet), qui décrit le système à analyser, l'arbre est alors construit de niveau en niveau en se demandant « quels sont les constituants de » chaque élément du niveau précédent, jusqu'à ce que les éléments les plus basiques soient atteints. La construction de l'arbre peut alors prendre fin lorsque les éléments matériels ont été suffisamment décrits d'après leurs rôles distincts dans la réalisation des fonctions identifiées dans les derniers niveaux de l'arbre des fonctions. En accord avec le degré de détail utilisé pour les analyses, trois niveaux sont considérés dans la suite : *système*, pour le système dans son ensemble qui est à analyser ; *sous-systèmes*, pour n'importe quel ensemble de composants regroupés selon des critères physiques ou fonctionnels ; et *unités de base*, pour les éléments considérés comme les plus basiques pour les analyses. Pour les CTI, les éléments matériels présentés dans la Section I.3.1.2, et la Figure III.1.3, peuvent être utilisés afin d'identifier certains éléments spécifiques. De par la construction de l'arbre, les relations entre un objet et ses parties sont uniquement définies par des relations logiques de type « et », ce qui signifie que chaque élément matériel est constitué de ses sous-parties.

Tout comme pour l'arbre des fonctions, différents types d'éléments matériels peuvent être distingués et, dans l'approche proposée, deux types sont utilisés : *éléments matériels principaux* et *éléments matériels de support*. Les sous-systèmes et unités de base sont des éléments matériels principaux car ils découlent directement de la décomposition du système. Les éléments matériels de support sont quant à eux des parties communes à, ou requises par, plusieurs éléments matériels principaux. (Dans l'exemple de la Figure III.1.3, plusieurs unités de base partagent le même support de communication interne, et toutes les unités de base utilisent la même alimentation). Dans la suite, des matrices de relations sont utilisées pour représenter les relations entre les éléments matériels de support et les éléments matériels principaux.

III.1.2.2.3. Liste des défauts et des défaillances

Dans la perspective d'effectuer des analyses de sûreté de fonctionnement, les défauts et les défaillances sont introduits dans une troisième partie du modèle, ce qui permet d'y intégrer les *aspects dysfonctionnels*. Cette partie n'est pas représentée sur la Figure III.1.3, mais est décrite à l'aide d'un exemple sur la Figure III.1.4. (En effet, il a été jugé irréaliste d'envisager une liste exhaustive de tous les défauts et les défaillances d'un système, sans prendre en compte les spécificités de celui-ci, de ses composants, et des applications considérées). Il s'agit d'une liste qui contient tous les défauts et les défaillances potentiels pouvant concerner au moins un des éléments matériels identifié dans les derniers niveaux de l'arbre des éléments matériels.

« Défaut » est ici utilisé comme synonyme de « anomalie » tel que défini par la norme CEI 61508 [IEC10] (cf. Section I.3.2.1), c'est-à-dire une condition anormale qui peut entraîner une réduction de capacité, ou la perte de capacité, d'une unité fonctionnelle (élément matériel) à réaliser une fonction requise ; et une défaillance est la cessation de cette aptitude. En accord avec ces définitions, un défaut est donc « antérieur » à une défaillance car il peut, ou non, conduire à une

défaillance, selon les effets engendrés sur les fonctions du système. Des définitions contradictoires ont cependant été données dans d'autres normes [IEC90]. Dans la suite, la norme CEI 61508 sera utilisée comme référence. En étudiant les réalisations de différentes fonctions (selon les exigences définies), des modes de défaillance peuvent ensuite être identifiés, c'est-à-dire qu'une description du défaut ou de la défaillance peut être donnée (comment celle-ci ou celui-ci est observé) [MRa96]. Le terme « mode de défaillance » peut alors être utilisé à différent niveaux. Par exemple, un mode de défaillance relatif à un niveau inférieur (par exemple, pour une unité de base) implique des effets qui constituent ensuite un mode de défaillance relatif à un niveau supérieur (par exemple, pour un sous-système) [MRa96]. Dans la suite, le terme « mode de défaillance » fera exclusivement référence aux fonctions globales du système (c'est-à-dire relatives au système dans son ensemble), identifiées dans l'arbre des fonctions.

Les défauts et les défaillances peuvent être identifiés selon différentes catégories et degrés de détail. M. Rausand *et al.* ont présenté les concepts de base de l'analyse des défaillances [MRa96], fournissant ainsi des outils utiles à l'identification et à la classification des défauts et des défaillances. Pour le modèle proposé, une approche déductive peut être utilisée afin d'identifier les défauts ou défaillances pouvant concerner chacun des éléments matériels identifiés dans les derniers niveaux de l'arbre des éléments matériels. (Contrairement aux AMDEC, les effets de ces défauts ou défaillances ne sont pas analysés à cette étape du modèle.) Pour des systèmes relatifs à la sécurité, une distinction peut être faite entre les *défaillances systématiques* et *aléatoires*. Une défaillance systématique est liée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés ; tandis qu'une défaillance dite « aléatoire » se produit à un instant aléatoire, et est liée à divers mécanismes de dégradation au sein du matériel [IEC10]. Par nature, les défaillances aléatoires sont souvent les plus appropriées pour effectuer des analyses de fiabilité lorsque des probabilités de défaillance sont évaluées. Cependant, des défaillances systématiques peuvent également être intégrées au modèle afin d'analyser les effets de celles-ci sur la réalisation des fonctions du système. Pour les systèmes relatifs à la sécurité, l'étude de ces effets peut alors aussi permettre de classer une défaillance comme étant *dangereuse* (c'est-à-dire qui a le potentiel de mettre le système dans un état dangereux ou dans un état qui ne lui permet pas d'accomplir sa ou ses fonctions de sécurité), ou *en sécurité*.

Un défaut ou une défaillance fait ainsi référence à des réalisations de fonctions, par l'intermédiaire d'éléments matériels. En accord avec cette logique, l'approche proposée intègre dans le modèle les défauts et les défaillances, d'abord par des relations entre ceux-ci et les éléments matériels, puis par des relations entre les éléments matériels et les fonctions. Ces deux ensembles de relations sont représentées par des matrices de relations, qui sont présentées dans la section suivante. Une fois la modélisation terminée, des analyses de relations pourront alors être effectuées afin d'identifier les effets de n'importe quel défaut ou défaillance sur les réalisations des fonctions du système, par l'intermédiaire des éléments matériels. Il n'est ainsi pas du ressort de cette étape de la modélisation de définir lequel des termes « défaut » ou « défaillance » est le plus approprié, et quels sont les modes de défaillance correspondants.

III.1.2.2.4. Matrices de relations

Les matrices de relations représentent les *aspects comportementaux* du système. Elles permettent ainsi de montrer comment chaque fonction peut être réalisée, selon les éléments matériels et les autres fonctions (par exemple, les fonctions de support). Dans l'approche proposée, elles permettent également de montrer comment chaque fonction peut ne pas être réalisée lors de l'occurrence d'un ou de plusieurs défauts et/ou défaillances. Le lien entre l'arbre des fonctions, l'arbre des éléments

matériels, et les défauts et défaillances est apporté par des matrices de relations définies entre : unités de base (éléments matériels principaux) et fonctions de base (fonctions principales), unités de base et fonctions de support, défauts et défaillance et unités de base, défauts et défaillances et éléments matériels de support. Ces *relations directes* sont qualifiées d' « *inter-parties* » car elles sont établies entre différentes parties du modèle. De plus, de par la construction de l'arbre des fonctions et de l'arbre des éléments matériels, ces matrices de relations sont uniquement utilisées entre des éléments de derniers niveaux (fonctions de base, fonctions de support, unités de base, éléments matériels de support, défauts et défaillances). En outre, parce que les relations entre les éléments matériels de support et les fonctions de base ou de support ne sont souvent pas directes, les matrices de relations correspondantes ne sont pas utilisées. (Des *relations indirectes* peuvent cependant exister par l'intermédiaire des éléments matériels principaux). Enfin, des *relations directes* et « *intra-partie* » (c'est-à-dire entre éléments d'une même partie du modèle) sont également définies entre : fonctions de support et fonctions de base, éléments matériels de support et unités de base.

Différent types de relations peuvent être utilisés dans les matrices de relations afin de définir le comportement du système. Par exemple, M. Modarres *et al.* ont proposé l'utilisation de relations [MMo99] : *logiques*, pour montrer les connections entre éléments ; *physiques*, pour intégrer des lois physiques ; et *floues*, en cas d'incertitudes. Afin de représenter la dynamique de certains systèmes (c'est-à-dire comment ils agissent et réagissent lors de changements dans leurs environnements), des relations *floues* et *dépendantes du temps* ont également été développées [YHu96, YHu99]. Enfin, d'autres types de relations ont été proposés dans une optique de sûreté de fonctionnement : *qualitative*, pour des analyses préliminaires en utilisant uniquement des relations descriptives ; *architecturales*, pour modéliser de façon déterministe les exigences de chaque élément vis-à-vis des autres éléments ; et *stochastiques*, pour représenter les effets indéterminés d'occurrences de défauts et de défaillances, d'états défaillants d'éléments matériels, et de dysfonctionnements de fonctions, sur les autres éléments [FBr09c]. À cette étape du modèle, des relations qualitatives sont utilisées (aucune valeur numérique n'est utilisée). Dans la suite, des relations stochastiques sont introduites afin d'effectuer des analyses de relations, notamment parce que ces dernières fournissent un moyen de prendre en compte des comportements mal connus du système.

Les composantes des matrices de relations sont alors représentées par des cercles pleins. De plus, une représentation étendue est proposée afin de définir des degrés de relations par l'utilisation de différentes couleurs (ainsi, il s'agit plus d'une modélisation « semi-qualitative »). L'objectif de cette représentation est de prendre en compte des comportements indéfinis du système. En effet, une relation entre deux éléments peut être indéterminée à cause de la complexité du système, par exemple due à la présence d'unités programmables ou de logiciels. Les couleurs des cercles dépendent alors du degré de relation entre l'élément aval (à gauche de la matrice) et l'élément amont (au dessus de la matrice). Un cercle coloré en noir signifie que l'élément amont nécessite toujours directement les pleines conditions opérationnelles des éléments aval associés pour être lui-même en état opérationnel. Un cercle coloré en plus clair signifie que l'élément amont peut être en état opérationnel même si les éléments aval associés ne sont pas dans des conditions pleinement opérationnelles (dans certains cas, ces conditions opérationnelles sont, de plus, indéterminées). Enfin, l'absence de cercle signifie qu'aucune relation directe entre les éléments n'est considérée.

III.1.3. Cas d'Étude : Capteur-Transmetteur de Gaz

Un capteur-transmetteur qui mesure la concentration de gaz par absorption infrarouge est utilisé comme cas d'étude. Le modèle « 3-Step » a été appliqué à ce système et est décrit sur la Figure

III.1.4. Le capteur-transmetteur est constitué de deux unités infrarouges : une *unité infrarouge de travail* qui émet un rayon dont la longueur d'onde est proportionnelle à la concentration du gaz à mesurer ; et une *unité infrarouge de référence* qui émet un rayon indépendant de la concentration de gaz. Ces rayons traversent une vitre de protection, et sont ensuite réfléchis par un miroir (les *optiques*). Par un rapport des longueurs d'onde des deux rayons reçus, la mesure de la concentration de gaz est obtenue avec une correction de l'obstruction (encrassage) des optiques, et des fluctuations de la puissance des rayons. Lorsqu'un certain seuil d'obstruction est dépassé (par exemple, dû à de la buée, de la poussière, ou à des dépôts sur les optiques), ces corrections ne sont plus suffisantes et des informations de diagnostic sont transmises. De plus, des éléments de chauffage des optiques permettent de prévenir l'apparition de buée. Parce que la température influe la mesure de la concentration de gaz, des *capteurs de température* (internes et externes) sont utilisés afin d'effectuer numériquement des compensations. Lorsque les températures sont en dehors des limites acceptables, cette compensation n'est plus adaptée et des informations de diagnostic sont transmises. Une *carte numérique* effectue l'ensemble des traitements des données, et contrôle les autres unités. Enfin, les principaux éléments du système partagent la même *alimentation*, et un *convertisseur* est, de plus, utilisé par les unités infrarouges. Ces éléments matériels sont décrits dans l'arbre des éléments matériels de la Figure III.1.4.

Les fonctions du système étudié sont les suivantes : *mesurer*, c'est-à-dire évaluer la concentration de gaz avec les corrections numériques adéquates ; *diagnostiquer*, c'est-à-dire vérifier que les facteurs influençant les mesures (obstruction des optiques, puissances des rayons, températures) sont dans des limites acceptables ; *auto-ajuster* (le zéro et le gain) afin de définir des paramètres numériques requis par les précédentes fonctions. Les fonctions *mesurer* et *diagnostiquer* consistent à *obtenir* puis à *traiter les données* appropriées. La communication avec le ou les systèmes externes est gérée par une carte analogique, mais n'est pas prise en compte dans ce cas d'étude. La fonction d'objectif est donc *obtenir des résultats de mesure et des informations de diagnostic*. Ces fonctions sont décrites dans l'arbre des fonctions de la Figure III.1.4.

Les relations directes intra et inter-parties entre les éléments matériels et les fonctions sont représentées par des matrices de relations. Par exemple, les capteurs de température sont quasi systématiquement requis pour l'auto-ajustage (de par les algorithmes d'auto-ajustage du zéro et du gain qui exploitent la température en tant que paramètre indispensable), tandis que dans certains cas, un état défaillant de ces capteurs de température permet toujours d'obtenir des données suffisantes de mesure (par exemple, lorsque la compensation de la température n'est pas déterminante). De même, selon l'état défaillant de la carte numérique, celui-ci peut impliquer directement un dysfonctionnement du traitement des données de diagnostic, ou des erreurs d'auto-ajustage qui peuvent ensuite également affecter le traitement des données de diagnostic en tant que relation indirecte.

Une liste simplifiée de neuf défauts et défaillances est donnée. Ceux-ci peuvent affecter un seul élément (par exemple, l'obstruction des optiques), ou plusieurs (par exemple, un défaut ou une défaillance commune aux deux unités infrarouges). À noter que certains défauts ou défaillances ont des conséquences indéterminées sur les éléments matériels, par exemple, à cause d'imprécisions dans les définitions (par exemple, des erreurs de logiciel au sein de la carte numérique qui peuvent affecter uniquement le contrôle de certains éléments), ou de contraintes environnementales difficiles à prédire à tout instant (notamment, la perte du chauffage des optiques peut ne pas avoir d'effets significatifs si, à ce moment, la température et l'humidité sont dans des conditions acceptables).

Certains éléments de la Figure III.1.4 (les « résultats des analyses de relations » et les représentations des incertitudes) correspondent aux analyses présentées dans la Section III.2.

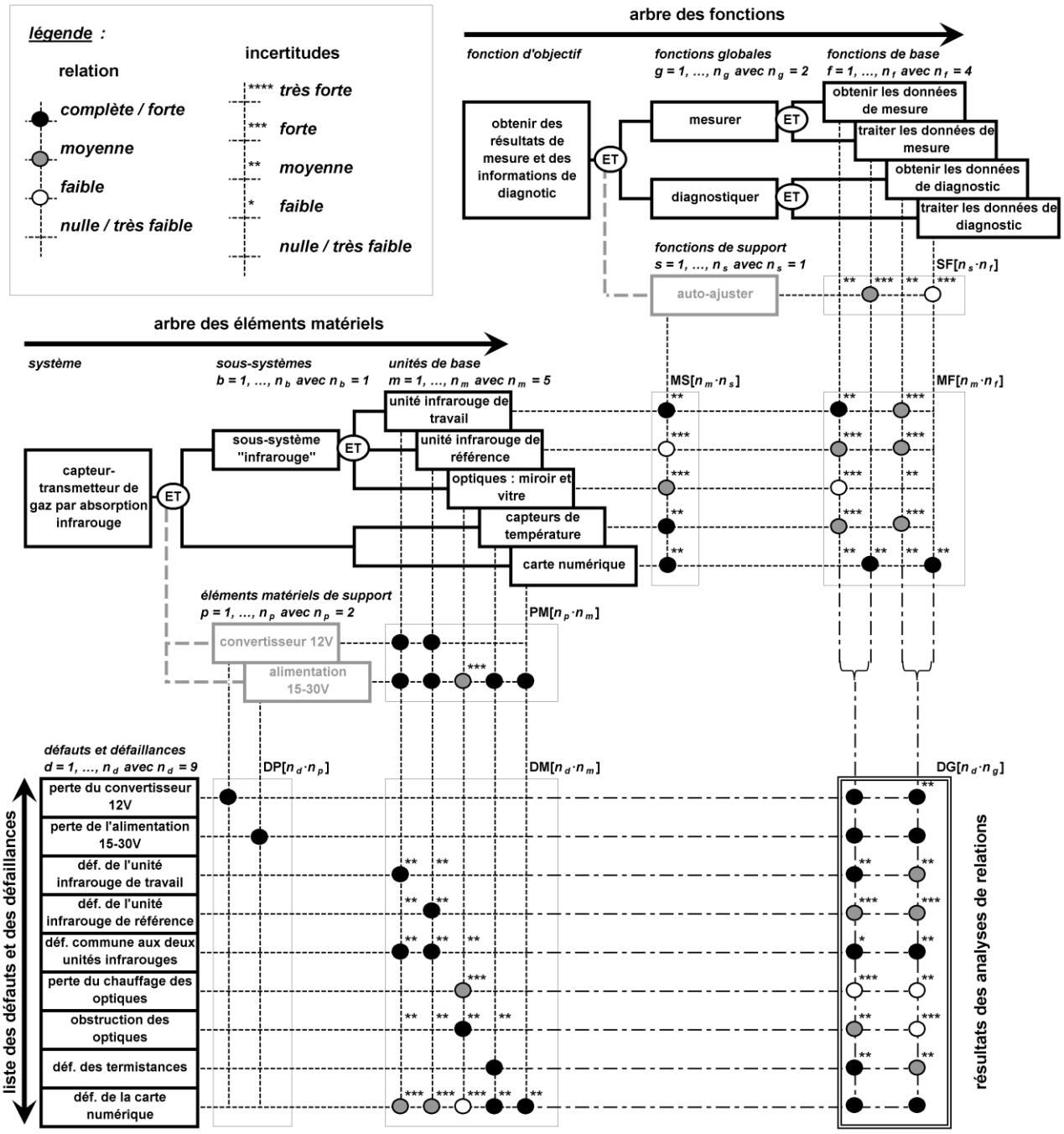

Figure III.1.4. Modèle « 3-Step » appliqué à un capteur-transmetteur de gaz par absorption infrarouge

III.2. ÉVALUATION DES « CAPTEURS-TRANSMETTEURS INTELLIGENTS »

III.2.1. Analyses de Fiabilité à partir du Modèle « 3-Step »

III.2.1.1. Analyses de relations

Les analyses de relations ont pour objectif d'évaluer les relations totales entre n'importe quel élément (défauts et défaillances, éléments matériels, fonctions), en y incluant les relations directes et indirectes. Pour cela, des relations stochastiques sont utilisées et, afin de manipuler de telles relations, celles-ci sont définies par des évènements. Tout d'abord, les *évènements de défectuosité* suivants sont définis :

D_d = {occurrence du défaut ou de la défaillance *d*} avec $d = 1, \ldots, n_d$
P_p = {état défaillant de l'élément matériel de support *p*} avec $p = 1, \ldots, n_p$
M_m = {état défaillant de l'unité de base (élément matériel principal) *m*} avec $m = 1, \ldots, n_m$
S_s = {dysfonctionnement de la fonction de support *s*} avec $s = 1, \ldots, n_s$
F_f = {dysfonctionnement de la fonction de base (fonction principale) *f*} avec $f = 1, \ldots, n_f$
G_g = {dysfonctionnement de la fonction globale (fonction principale) *g*} avec $g = 1, \ldots, n_g$

Ensuite, des *évènements de relations* (directes, indirectes, ou totales) sont définis. En notation générale, l'évènement correspondant à une relation directe entre un élément aval nommé *a*, et un élément amont nommé *b*, est défini dans une matrice nommée AB, à la ligne indicée par *a* et la colonne indicée par *b*, tel que :

$AB_{a,b}$ = {l'évènement A_a implique directement (c'est-à-dire inconditionnellement aux autres évènements) l'évènement B_b}

Les *évènements de relations directes* suivants sont donc définis :

$DP_{d,p}$ = {l'occurrence du défaut ou de la défaillance *d* implique directement un état défaillant de l'élément matériel de support *p*}
$DM_{d,m}$ = {l'occurrence du défaut ou de la défaillance *d* implique directement un état défaillant de l'unité de base *m*}
$PM_{p,m}$ = {un état défaillant de l'élément matériel de support *p* implique directement un état défaillant de l'unité de base *m*}
$MS_{m,s}$ = {un état défaillant de l'unité de base *m* implique directement un dysfonctionnement de la fonction de support *s*}
$MF_{m,f}$ = {un état défaillant de l'unité de base *m* implique directement un dysfonctionnement de la fonction de base *f*}
$SF_{s,f}$ = {un dysfonctionnement de la fonction de support *s* implique directement un dysfonctionnement de la fonction de base *f*}

L'hypothèse est faite que tous ces évènements sont indépendants (ce qui peut nécessiter certaines considérations, au préalable, lors de la modélisation du système, notamment quant au degré de détail utilisé). De plus, on attribue des probabilités d'occurrence de ces évènements de relations, notées de façon générale $P[AB_{a,b}]$, et dont les valeurs dépendent des couleurs des cercles présents dans les matrices de relations. Par exemple, le Tableau III.2.1 peut être utilisé pour traduire un degré de relation en une probabilité, et vice-versa.

D'autres relations entre éléments existent également. Par exemple, l'occurrence du défaut ou de la défaillance *d* (évènement D_d) peut directement impliquer un état défaillant de l'élément matériel de

support *p* (évènement P_p), si l'évènement $DP_{d,p}$ correspondant se produit, ainsi qu'un état défaillant de l'unité de base *m* (évènement M_m), si l'évènement $DM_{d,m}$ correspondant se produit. De plus, l'état défaillant de ce même élément matériel de support *p* peut aussi directement impliquer l'état défaillant de cette même unité de base *m*, si l'évènement $PM_{p,m}$ correspondant se produit. L'état défaillant de l'unité de base *m*, dû à l'occurrence du défaut ou de la défaillance *d*, par l'intermédiaire de l'état défaillant de l'élément matériel de support *p* (lorsque les évènements $DP_{d,p}$ et $MP_{m,p}$ correspondants se produisent tous les deux), est alors un *évènement de relations indirectes*. Les évènements de relations indirectes sont ainsi des combinaisons d'évènements de relations directes. De plus, parce que les évènements de relations directes sont indépendants, les évènements de relations directes et indirectes ne sont pas incompatibles. Par convenance, seules les relations directes doivent être définies dans le modèle « 3-Step ». Les relations totales, prenant en compte toutes les relations directes et indirectes, sont ensuite obtenues par les expressions décrites ci-après.

Les *évènements de relations totales* définis entre les défauts et défaillances et les unités de base sont :

$DMtot_{d,m}$ = {l'occurrence du défaut ou de la défaillance *d* implique (directement ou indirectement) un état défaillant de l'élément de base *m*}

avec :

$$DMtot_{d,m} = \{DM_{d,m} \cup_p (DP_{d,p} \cap PM_{p,m})\} \quad \text{[III.2.1]}$$

Les *évènements de relations totales* définis entre les unités de base et les fonctions de base sont :

$MFtot_{m,f}$ = {un état défaillant de l'élément de base *m* implique (directement ou indirectement) un dysfonctionnement de la fonction de base *f*}

avec :

$$MFtot_{m,f} = \{MF_{m,f} \cup_s (MS_{m,s} \cap SF_{s,f})\} \quad \text{[III.2.2]}$$

Les *évènements de relations totales* définis entre les défauts et défaillances et les fonctions de base sont :

$DF_{d,f}$ = {l'occurrence du défaut ou de la défaillance *d* implique (directement ou indirectement) un dysfonctionnement de la fonction de base *f*}

avec :

$$DF_{d,f} = \{\cup_m (DMtot_{d,m} \cap MFtot_{m,f})\} \quad \text{[III.2.3]}$$

Il est souvent plus intéressant d'étudier les fonctions globales plutôt que les fonctions de base. Ainsi, les *évènements de relations totales* définis entre les défauts et défaillances et les fonctions globales sont :

$DG_{d,g}$ = {l'occurrence du défaut ou de la défaillance *d* implique (directement ou indirectement) un dysfonctionnement de la fonction globale *g*}

avec :

$$DG_{d,g} = \{\cup_{f \in E_g} DF_{d,f}\} \quad \text{[III.2.4]}$$

et E_g l'ensemble des fonctions de base *f* qui doivent être accomplies pour réaliser la fonction globale *g*.

Il est alors possible d'exprimer la probabilité de dysfonctionnement de la fonction globale *g* par :

$$P[G_g] = P[\cup_d (D_d \cap DG_{d,g})] \quad \text{[III.2.5]}$$

À noter que les évènements donnés dans les matrices DMtot (cf. Équation III.2.1) et MFtot (cf. Équation III.2.2) ne sont pas indépendants. En effet, de mêmes évènements $PM_{p,m}$ interviennent dans plusieurs lignes de la matrice DMtot, et de mêmes évènements $DP_{d,p}$ interviennent dans

plusieurs colonnes (respectivement pour des évènements $SF_{s,f}$ et $MS_{m,s}$ dans la matrice MFtot). Ainsi, certains évènements des matrices DF et DG ne sont pas indépendants, et les Équations III.2.3 et III.2.4 doivent être manipulées avec des approches appropriées, par exemple en utilisant des décompositions pivotales. Afin d'effectuer de telles analyses en utilisant des logiciels classiques de sûreté de fonctionnement, des arbres de défaillance équivalents peuvent être utilisés, tels que proposés sur la Figure III.2.1 pour les probabilités de dysfonctionnement des fonctions de base ($P[F_f]$), et sur la Figure III.2.2 pour les probabilités de dysfonctionnement des fonctions globales ($P[G_g]$). D'après l'Équation III.2.5, un moyen relativement simple de calculer les valeurs des relations totales est alors d'utiliser l'expression suivante :

$$P[DG_{d,g}] = P[G_g \mid (D_d \cap_{\delta \neq d} D_\delta^*)] \qquad \text{[III.2.6]}$$

avec D_δ^* qui représente la non-occurrence de l'évènement D_δ.

L'Équation III.2.6 signifie que, si l'occurrence du défaut ou la défaillance *d* (évènement D_d) se produit, et aucune autre occurrence de défaut ou de défaillance (ensemble des évènements D_δ^* tel que $\delta \neq d$), le dysfonctionnement de la fonction globale *g* (évènement G_g) se produit avec une probabilité égale à $P[DG_{d,g}]$. Cette valeur peut ainsi être interprétée comme l'effet individuel du défaut ou de la défaillance *d* sur la fonction globale *g*, pouvant alors jouer le rôle d'un « facteur d'importance ». À noter que les Équations III.2.5 et III.2.6 peuvent être transposées à n'importe quelle fonction de base *f*, en remplaçant les évènements G_g par F_f et les évènements $DG_{d,g}$ par $DF_{d,f}$.

III.2.1.2. Probabilités de dysfonctionnements et de modes de défaillance

Les probabilités de dysfonctionnements et de modes de défaillance sont évaluées d'après les hypothèses suivantes :

- les évènements de relations directes (évènements donnés dans les matrices DP, DM, PM, MS, MF, et SF) sont indépendants, et les probabilités de ces évènements sont indépendantes du temps (considérant alors que le comportement du système n'est pas « dynamique ») ;
- les occurrences des défauts et des défaillances (évènements D_d avec $d = 1, \ldots, n_d$) sont indépendants, et les probabilités de ces évènements sont dépendantes du temps et donc notées $P[D_d](t)$;
- aucune action de maintenance n'est considérée sur toute la période d'étude.

Les probabilités de dysfonctionnements des fonctions globales au temps *t*, ainsi notées $P[G_g](t)$, peuvent alors être évaluées, par exemple en utilisant une approche basée sur des arbres de défaillance équivalents comme proposés sur les Figures III.2.1 et III.2.2, ou en utilisant l'intervalle suivant basé sur les résultats des analyses de relations :

$$\sum_d (P[DG_{d,g}] \cdot P[D_d](t) \cdot \prod_{\delta \neq d} (1 - P[D_\delta](t))) \leq P[G_g](t) \leq \sum_d (P[DG_{d,g}] \cdot P[D_d](t)) \qquad \text{[III.2.7]}$$

La borne supérieure de cet intervalle est déduite de l'Équation III.2.5, et la borne inférieure de l'Équation III.2.6, en négligeant l'occurrence de plus d'un défaut ou défaillance (évènements D_d). À noter que l'Équation III.2.7 peut être transposée à n'importe quelle fonction de base *f*, en remplaçant les évènements G_g par F_f et les évènements $DG_{d,g}$ par $DF_{d,f}$.

Les modes de défaillance peuvent être définis par l'intermédiaire des combinaisons de réalisations des fonctions globales (en tenant compte des exigences de performance définis). Les probabilités des modes de défaillance au temps *t* peuvent alors être obtenues en utilisant, par exemple, une approche basée sur les arbres de défaillance, comme pour les précédentes évaluations.

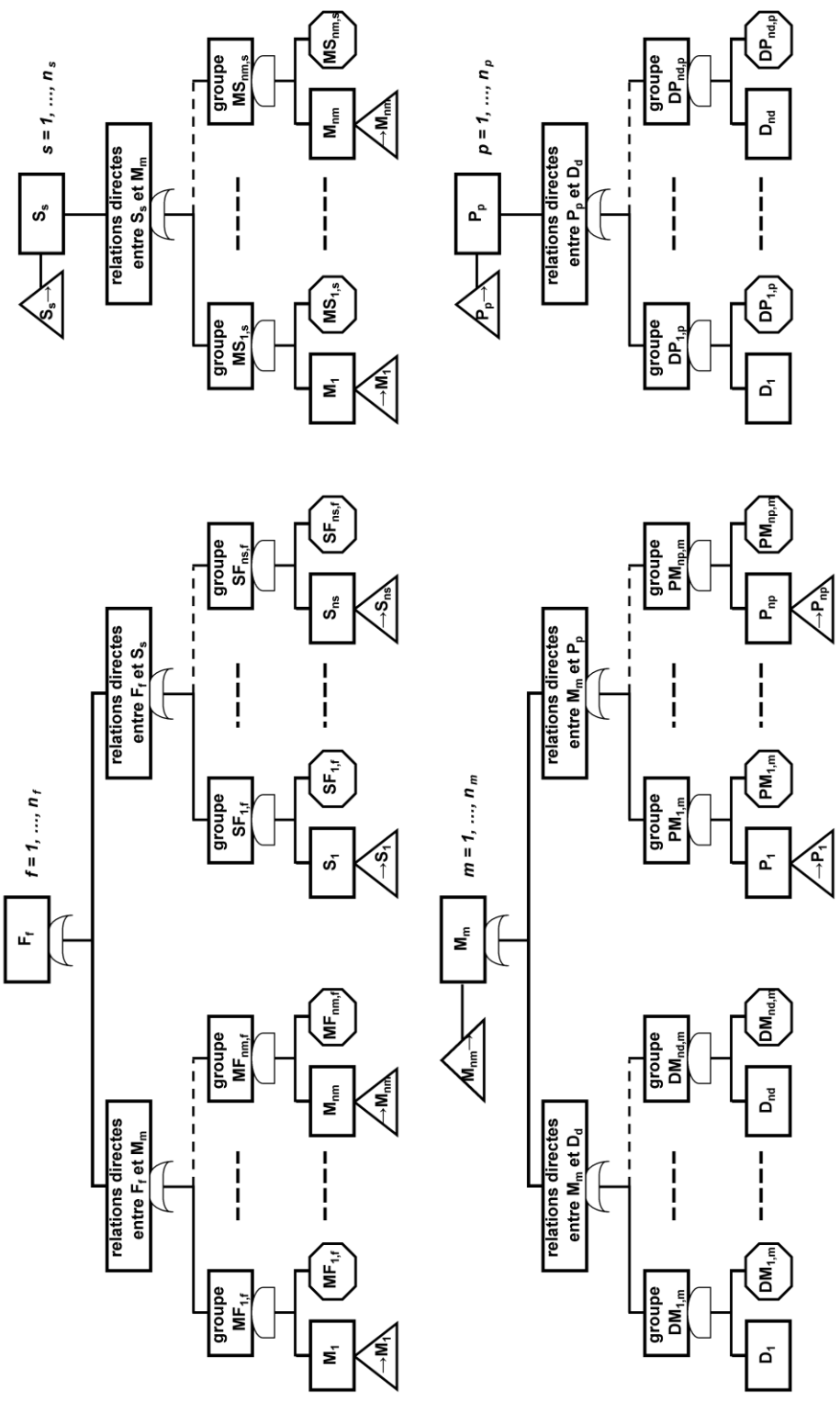

Figure III.2.1. Arbres de défaillance équivalents au modèle « 3-Step »

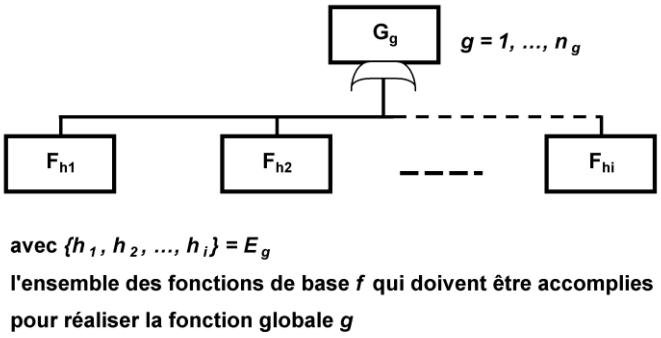

Figure III.2.2. Arbre de défaillance équivalent pour les fonctions globales *g*

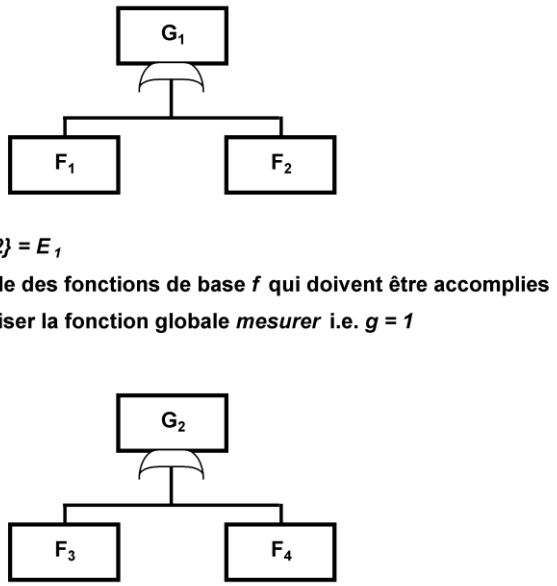

Figure III.2.3. Arbre de défaillance équivalent pour la fonction globale *mesurer* i.e. *g = 1*, et la fonction globale *diagnostiquer* i.e. *g = 2* (cf. Figure III.1.4)

III.2.1.3. Analyses d'incertitudes

La prise en compte des incertitudes liées aux données d'entrée est répandue dans les analyses de fiabilité, en revanche, la prise en compte des incertitudes liées au modèle l'est beaucoup moins (cf. Section I.2.1.3). Dans l'approche proposée, les relations entre les éléments constituent, par nature, une paramétrisation du modèle. Il est alors possible, dans une approche commune, d'effectuer à la fois des analyses d'incertitudes liées aux paramètres (par exemple, les taux de défaillance) et au modèle (par l'intermédiaire des relations entre les éléments). Par exemple, des lois Log-Normales sont généralement utilisées pour modéliser les taux de défaillance [GAp90] (données d'entrée pour les probabilités d'occurrence des défauts et des défaillances), et des lois Uniformes peuvent être utilisées pour modéliser les probabilités d'occurrence des évènements de relations directes, en tant que variables aléatoires. Une approche probabiliste est ainsi préférée car elle permet de disposer de critères quantitatifs, comme par exemple les moments de premier et de second ordre (dont les variances), qui peuvent être utilisés pour évaluer les incertitudes dans les résultats, et les comparer avec les incertitudes dans les données d'entrée. Les analyses d'incertitudes peuvent alors être effectuées sur les résultats des analyses de relations et sur ceux des probabilités de dysfonctionnements et de modes de défaillance, afin de tester la robustesse de l'approche proposée, notamment lorsque certains comportements du système sont mal connus.

III.2.2. Cas d'Étude : Capteur-Transmetteur de Gaz (Suite)

III.2.2.1. Analyses de relations appliquées au cas d'étude

Le capteur-transmetteur de gaz décrit par la Figure III.1.4 est ici repris. Les probabilités d'occurrence des évènements de relations directes sont : $P[\mathrm{DP}_{d,p}]$, $P[\mathrm{DM}_{d,m}]$, $P[\mathrm{PM}_{p,m}]$, $P[\mathrm{MS}_{m,s}]$, $P[\mathrm{MF}_{m,f}]$, et $P[\mathrm{SF}_{s,f}]$, avec $n_d = 9$, $n_p = 2$, $n_m = 5$, $n_s = 1$, et $n_f = 4$, les nombres respectifs de défauts et défaillances, d'éléments matériels de support, d'unités de base, de fonctions de support, et de fonctions de base. Ces derniers correspondent ainsi aux dimensions des matrices de relations DP, DM, PM, MS, MF, et SF, qui sont précisées entre crochets sur la Figure III.1.4.

D'après la Figure III.1.4, il est par exemple possible de voir qu'un état défaillant de l'élément matériel *carte numérique* (évènement M_5) implique directement un dysfonctionnement de la fonction de support *auto-ajuster* (évènement S_1), si l'évènement $MS_{5,1}$ se produit, et un dysfonctionnement de la fonction de base *traiter les données de mesure* (évènement F_2), si l'évènement $MF_{5,2}$ se produit. Il s'agit là d'exemples d'évènements de relations directes. De plus, un dysfonctionnement de la fonction *auto-ajuster* (évènement S_1) implique directement un dysfonctionnement de la fonction *traiter les données de mesure* (évènement F_2), si l'évènement $SF_{1,2}$ se produit. Le dysfonctionnement de la fonction *traiter les données de mesure*, dû à l'état défaillant de l'élément matériel *carte numérique*, par l'intermédiaire du dysfonctionnement de la fonction *auto-ajuster*, est quant à lui un exemple d'évènement de relation indirecte.

Les deux fonctions globales ($n_g = 2$) utilisées pour ce cas d'étude sont : *mesurer* (pour $g = 1$) et *diagnostiquer* (pour $g = 2$). D'après la Figure III.1.4, les relations totales entre les défauts et défaillances et ces fonctions globales sont, par application de l'Équation III.2.4, définies par :

$$\mathrm{DG}_{d,1} = \{\mathrm{DF}_{d,1} \cup \mathrm{DF}_{d,2}\} \qquad \text{[III.2.8]}$$

$$\mathrm{DG}_{d,2} = \{\mathrm{DF}_{d,3} \cup \mathrm{DF}_{d,4}\} \qquad \text{[III.2.9]}$$

Tableau III.2.1. Analyses de relations : données d'entrée et représentation graphique

relation	donnée d'entrée pour les probabilités d'occurrence des évènements de relations directes[a]	traduction graphique des résultats pour les probabilités d'occurrence des évènements de relations totales[b]
totale / forte	*1.000*	*0.833* à *1.000*
moyenne	*0.667*	*0.500* à *0.833*
faible	*0.333*	*0.167* à *0.500*
nulle / très faible	*0.000*	*0.000* à *0.167*

[a]Ces évènements sont ceux donnés dans les matrices DP, DM, PM, MS, MF, et SF.
[b]Ces évènements incluent notamment ceux donnés dans la matrice DG.

Tableau III.2.2. Analyses de relations : résultats[a] pour les fonctions globales

défaut ou défaillance *d*	effet individuel sur la fonction globale *mesurer* i.e. $P[DG_{d,1}]$	effet individuel sur la fonction globale *diagnostiquer* i.e. $P[DG_{d,2}]$
1	*1.000*	*0.926*
2	*1.000*	*1.000*
3	*1.000*	*0.778*
4	*0.741*	*0.704*
5	*1.000*	*0.926*
6	*0.420*	*0.148*
7	*0.630*	*0.222*
8	*0.889*	*0.778*
9	*1.000*	*1.000*

[a]Ces résultats ont été obtenus en utilisant des arbres de défaillance équivalents et l'Équation III.2.6.

Pour ce cas d'étude, les probabilités $P[DG_{d,g}]$ ont été obtenues en utilisant les arbres de défaillance équivalents décrits sur les Figures III.2.3 et III.2.1, et l'Équation III.2.6, calculés à l'aide de SimTree, le module d'analyses des arbres de défaillance du logiciel Aralia Workshop [Ara09, YDu97a]. Les données d'entrée utilisées pour les probabilités d'occurrence des évènements de relations directes (évènements donnés dans les matrices DP, DM, PM, MS, MF, et SF) sont données dans le Tableau III.2.1, d'après la Figure III.1.4. Par exemple, $SF_{1,2}$ représente un évènement correspondant à une relation moyenne, donc $P[SF_{1,2}] = 0.667$. De même, $P[MF_{m,2}] = 0.000$ pour $m = 1, \ldots, 4$, et $P[MF_{5,2}] = 1.000$, etc.

Les résultats des analyses de relations, relatives aux relations totales entre les défauts et défaillances et les fonctions globales (probabilités d'occurrence des évènements donnés dans la matrice DG), sont donnés dans le Tableau III.2.2, et traduits graphiquement sur la Figure III.1.4 (« résultats d'analyses de relations »), d'après le Tableau III.2.1. Par exemple, $P[DG_{8,2}] = 0.778$ et, d'après le Tableau III.2.1, $DG_{8,2}$ représente donc un évènement correspondant à une relation moyenne ce qui, d'après la légende de la Figure III.1.4, se traduit graphiquement par un cercle de couleur gris foncé. Une interprétation de ce résultat est « si l'occurrence d'un *défaut ou défaillance des thermistances* se produit, et aucune autre occurrence de défaut ou de défaillance, alors un dysfonctionnement de la fonction globale *diagnostiquer* se produira avec une probabilité égale à *0.778* ».

III.2.2.2. Probabilités de dysfonctionnements et de modes de défaillance appliquées au cas d'étude

Les probabilités de dysfonctionnements et de modes de défaillance pour le cas d'étude sont évaluées en utilisant les données suivantes :

- les probabilités d'occurrence des évènements de relations directes (évènements donnés dans les matrices DP, DM, PM, MS, MF, et SF) sont données dans le Tableau III.2.1, en accord avec la Figure III.1.4 (tout comme pour les analyses de relations, cf. Section III.2.2.1) ;
- les probabilités d'occurrence des défauts et des défaillances (évènements D_d) au temps *t* sont exprimées dans le Tableau III.2.3.

Les probabilités d'occurrences des défauts et des défaillances au temps *t* (cf. Tableau III.2.3), notées $P[D_d](t)$, prennent en compte la structure interne des éléments matériels, qui ne sont pas visibles sur la Figure III.1.4, en accord avec le niveau de décomposition utilisé. Par exemple, les thermistances sont au nombre de deux, et sont redondantes ($P[D_8](t)$ correspond à une fonction de défiabilité pour une structure en *1*-sur-*2* [MRa02]). De plus, trois éléments de chauffage des optiques sont utilisés, et il est considéré que leur fonction est réalisée selon une structure en *2*-sur-*3* (cf. $P[D_6](t)$ dans le Tableau III.2.3). L'incertitude liée à cette structure est alors prise en compte par l'intermédiaire de la relation qui représente un effet indéterminé du défaut ou défaillance *perte du chauffage des optiques*, sur l'unité de base *optiques* ($P[DM_{6,3}] = 0.667$ d'après la Figure III.1.4 et le Tableau III.2.1).

L'approche « exacte » obtenue à partir des arbres de défaillance équivalents des Figures III.2.3 et III.2.1 a permis d'obtenir les résultats suivants à partir de l'Équation III.2.5 : $P[G_1](60 \text{ jours}) = 4.31 \cdot 10^{-3}$ et $P[G_2](60 \text{ jours}) = 2.38 \cdot 10^{-3}$, qui sont respectivement les probabilités de dysfonctionnements des fonctions globales *mesurer* et *diagnostiquer* ; et l'Équation III.2.7 fournit des encadrements précis de ces valeurs, respectivement : $[4.30 \cdot 10^{-3} ; 4.32 \cdot 10^{-3}]$ et $[2.37 \cdot 10^{-3} ; 2.38 \cdot 10^{-3}]$. $P[G_1](t)$ et $P[G_2](t)$ sont représentées sur la Figure III.2.4.

Tableau III.2.3. Probabilités de dysfonctionnements et de modes de défaillance : données d'entrée pour les défauts et les défaillances

défaut ou défaillance *d*	probabilité d'occurrence du défaut ou de la défaillance *d* au temps *t* i.e. $P[D_d](t)$	taux de défaillance i.e. λ_d [heure^{-1}]
1	$1 - exp(-\lambda_1 \cdot t)$	$5 \cdot 10^{-8}$
2	$1 - exp(-\lambda_2 \cdot t)$	$5 \cdot 10^{-8}$
3	$1 - exp(-\lambda_3 \cdot t)$	$4 \cdot 10^{-7}$
4	$1 - exp(-\lambda_4 \cdot t)$	$4 \cdot 10^{-7}$
5	$1 - exp(-\lambda_5 \cdot t)$	$1 \cdot 10^{-7}$
6	$1 - 3 \cdot exp(-2 \cdot \lambda_6 \cdot t) + 2 \cdot exp(-3 \cdot \lambda_6 \cdot t)$	$3 \cdot 10^{-6}$
7	$1 - exp(-\lambda_7 \cdot t)$	$3 \cdot 10^{-6}$
8	$1 - 2 \cdot exp(-\lambda_8 \cdot t) + exp(-2 \cdot \lambda_8 \cdot t)$	$5 \cdot 10^{-7}$
9	$1 - exp(-\lambda_9 \cdot t)$	$2 \cdot 10^{-7}$

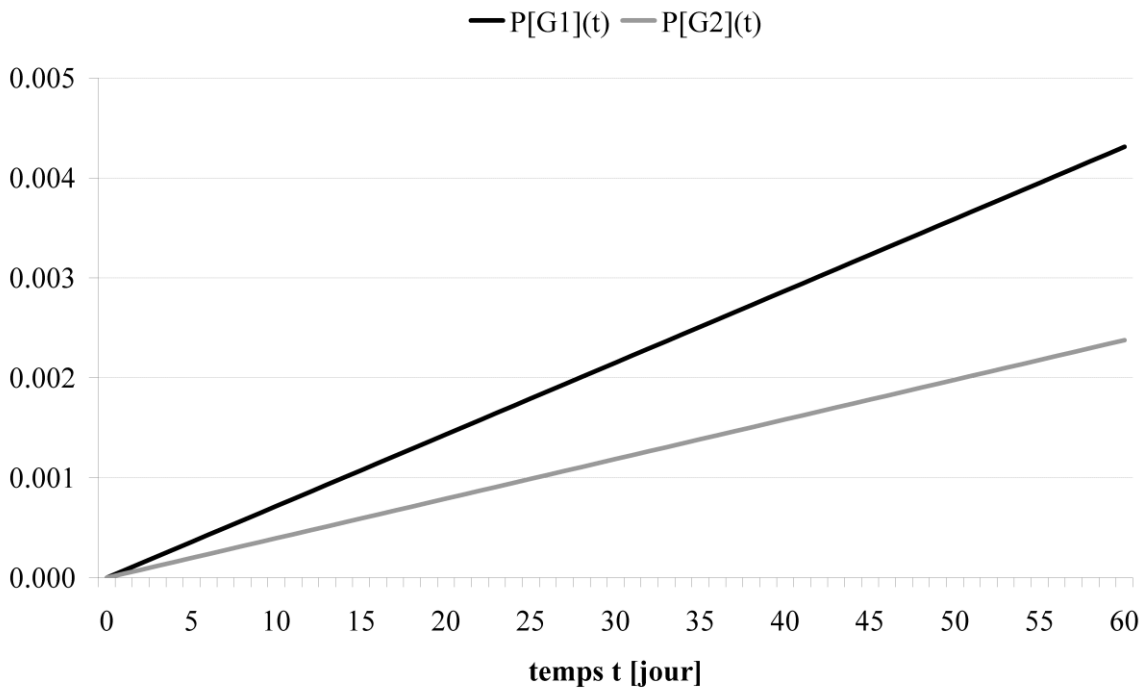

Figure III.2.4. Probabilités de dysfonctionnements de la fonction globale *mesurer* i.e. $P[G_1](t)$, et de la fonction globale *diagnostiquer* i.e. $P[G_2](t)$

Tableau III.2.4. Définitions des modes de défaillance

mode de défaillance	réalisation de la fonction globale *mesurer* i.e. *g = 1*	réalisation de la fonction globale *diagnostiquer* i.e. *g = 2*
$MoDe_0$	fonctionnement i.e. G_1*	fonctionnement i.e. G_2*
$MoDe_1$	fonctionnement i.e. G_1*	dysfonctionnement i.e. G_2
$MoDe_2$	dysfonctionnement i.e. G_1	fonctionnement i.e. G_2*
$MoDe_3$	dysfonctionnement i.e. G_1	dysfonctionnement i.e. G_2

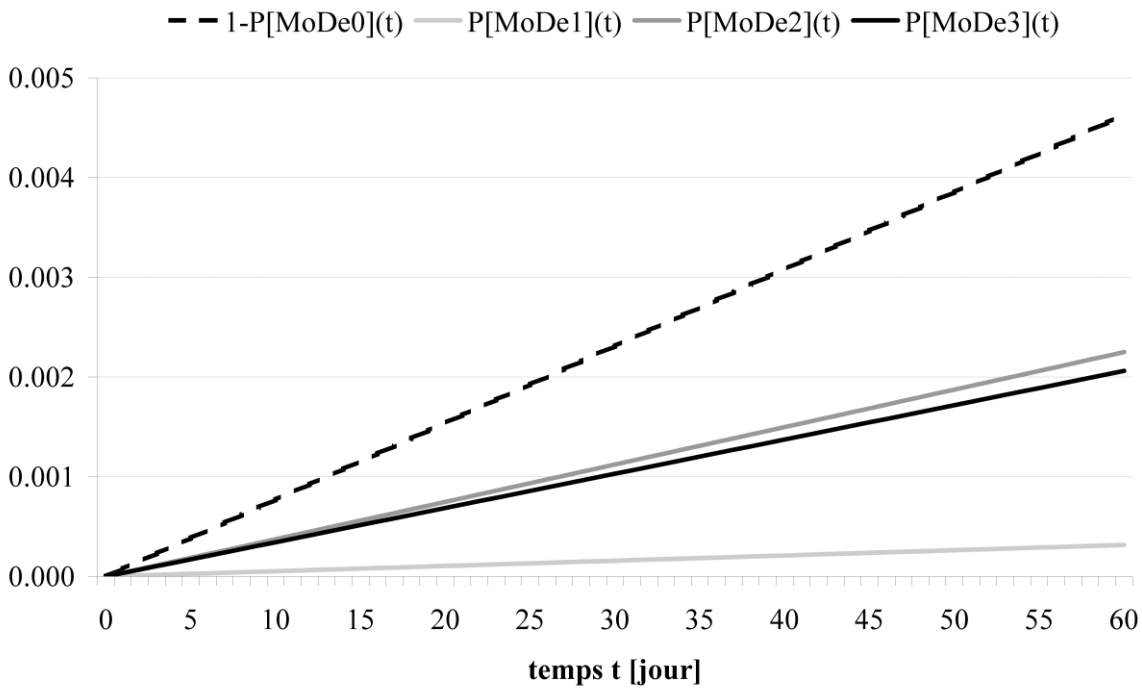

Figure III.2.5. Probabilités des modes de défaillance (cf. Tableau III.2.4)

Les modes de défaillance du cas d'étude sont définis dans le Tableau III.2.4. En accord avec l'approche proposée, l'exactitude des données transmises par le capteur-transmetteur de gaz dépend des réalisations des fonctions correspondantes. Par exemple, si la fonction globale *mesurer* fonctionne et la fonction globale *diagnostiquer* dysfonctionne, alors le système est capable d'obtenir des résultats de mesure correctes mais pas des informations de diagnostic correctes, et ce mode de défaillance est noté $MoDe_1$. Le mode de défaillance réciproque est noté $MoDe_2$. $MoDe_3$ correspond à la situation où ni la fonction *mesurer*, ni la fonction *diagnostiquer* ne fonctionnent, et $MoDe_0$ à la situation où les deux fonctionnent ($MoDe_0$ n'est donc pas littéralement un « mode de défaillance »).

Les probabilités de modes de défaillance au temps *t* ont été obtenues par une approche basée sur des arbres de défaillance équivalents, similaire à celle des analyses précédentes, et les résultats sont représentés sur la Figure III.2.5 (pour des raisons d'échelle et d'orientation « défaillance », cette figure représente $1 - P[MoDe_0](t)$ à la place de $P[MoDe_0](t)$). Par exemple, il peut être déduit de ces résultats que, lorsque la fonction *diagnostiquer* dysfonctionne ($MoDe_1$ ou $MoDe_3$), il est plus probable que la fonction *mesurer* dysfonctionne également ($P[MoDe_3](t) > P[MoDe_1](t)$). À l'inverse, lorsque la fonction *mesurer* dysfonctionne ($MoDe_2$ ou $MoDe_3$), la fonction *diagnostiquer* fonctionne ou dysfonctionne avec une probabilité presque égale ($P[MoDe_2](t) \approx P[MoDe_3](t)$). La fonction *mesurer* « couvre » donc une plus grande partie des défauts et défaillances.

III.2.2.3. Analyses d'incertitudes appliquées au cas d'étude

Afin d'effectuer les analyses d'incertitudes à la fois liées aux paramètres et au modèle (relatives aux comportements du système), et ensuite d'être en mesure d'évaluer les contributions respectives de ces incertitudes d'entrée sur les résultats, trois cas sont considérés :

i. incertitudes dans les relations uniquement (incertitudes liées au modèle), c'est-à-dire que lorsqu'une ou plusieurs étoiles sont attribuées à une relation directe sur la Figure III.1.4, la valeur de cette relation n'est plus définie par le Tableau III.2.1, mais est une variable aléatoire distribuée selon une loi Uniforme telle que définie dans le Tableau III.2.5 ;
ii. incertitudes dans les défauts et défaillances uniquement (incertitudes liées aux paramètres), c'est-à-dire que les taux de défaillance ne sont plus définis par le Tableau III.2.3 (dernière colonne), mais sont des variables aléatoires distribuées selon des lois Log-Normales telles que les moyennes sont égales aux valeurs initiales des taux de défaillance donnés dans le Tableau III.2.3, et les facteurs d'erreur sont égaux à *5* (les bornes inférieures et supérieures de l'intervalle de confiance centré et à *90*% sont respectivement obtenues en divisant et en multipliant la valeur médiane par *5*) ;
iii. incertitudes dans les relations et dans les défauts et défaillances (incertitudes liées au modèle et aux paramètres).

Pour les cas i et iii, les propriétés (espérances et variances) des variables aléatoires décrivant les relations directes sont données dans le Tableau III.2.5. Pour les cas ii et iii, les probabilités d'occurrences des défauts et de défaillances au temps *t* ($P[D_d](t)$) sont alors des variables aléatoires, et leurs propriétés au temps $t = 60$ jours sont données dans le Tableau III.2.6. À noter que les variances de $P[D_d](t)$ sont plus faibles que les variances des valeurs de relations directes, sur toute la période *[0 ; 60* jours*]*, c'est-à-dire que, pour les données d'entrée, de plus fortes incertitudes sont considérées pour les relations que pour les défauts et les défaillances. Les incertitudes, d'après les variances, sont traduites graphiquement par des étoiles sur la Figure III.1.4, d'après le Tableau III.2.7. Rappelons que des certaines relations directes, celles qui ne sont pas marquées par une ou

Tableau III.2.5. Analyses d'incertitudes : données d'entrée pour les valeurs de relations

relation	distribution[a,b,c]	espérance	variance
totale / forte	U[*0.833* ; *1.000*]	*0.917*	$2.31 \cdot 10^{-3}$
moyenne	U[*0.500* ; *8.333*]	*0.667*	$9.26 \cdot 10^{-3}$
faible	U[*0.167* ; *0.500*]	*0.333*	$9.26 \cdot 10^{-3}$
nulle / très faible	U[*0.000* ; *0.167*]	*0.083*	$2.31 \cdot 10^{-3}$

[a]Lorsqu'une relation est « certaine » (non marquée par une ou des étoiles sur la Figure III.1.4), les données du Tableau III.2.1 s'appliquent toujours.
[b]U[*a* ; *b*] est une loi Uniforme continue entre la valeur *a* et la valeur *b*.
[c]Plus une relation est définie comme « extrême » (forte ou très faible), plus l'incertitude est considérée comme faible, d'après les variances.

Tableau III.2.6. Analyses d'incertitudes : données d'entrée pour les défauts et les défaillances

défaut ou défaillance *d*	probabilité[a] d'occurrence du défaut ou de la défaillance *d* au temps *t = 60* jours i.e. $P[\mathrm{D_d}](60$ jours$)$	
	espérance i.e. $E[P[\mathrm{D_d}](60$ jours$)]$	variance i.e. $V[P[\mathrm{D_d}](60$ jours$)]$
1	$7.17 \cdot 10^{-5}$	$4.85 \cdot 10^{-9}$
2	$7.18 \cdot 10^{-5}$	$4.86 \cdot 10^{-9}$
3	$5.75 \cdot 10^{-4}$	$3.16 \cdot 10^{-7}$
4	$5.75 \cdot 10^{-4}$	$3.26 \cdot 10^{-7}$
5	$1.44 \cdot 10^{-4}$	$1.99 \cdot 10^{-8}$
6	$5.52 \cdot 10^{-5}$	$4.64 \cdot 10^{-9}$
7	$4.32 \cdot 10^{-3}$	$1.80 \cdot 10^{-5}$
8	$5.17 \cdot 10^{-7}$	$7.85 \cdot 10^{-13}$
9	$2.89 \cdot 10^{-4}$	$8.17 \cdot 10^{-8}$

[a]Ces résultats ont été obtenus d'après *100 000* de simulations de Monte Carlo pour chaque ligne, en utilisant les expressions données dans le Tableau III.2.3 (seconde colonne), lorsque les taux de défaillance suivent des lois Log-Normales de moyennes égales à λ_d (cf. Tableau III.2.3, troisième colonne) et de facteurs d'erreur égaux à *5*.

Tableau III.2.7. Analyses d'incertitudes : représentation graphiques

incertitude	représentation graphique	variance correspondante
très forte	****	supérieure à $5.10 \cdot 10^{-2}$
forte	***	$5.10 \cdot 10^{-3}$ à $5.10 \cdot 10^{-2}$
moyenne	**	$5.10 \cdot 10^{-4}$ à $5.10 \cdot 10^{-3}$
faible	*	$5.10 \cdot 10^{-5}$ à $5.10 \cdot 10^{-2}$
très faible		inférieure à $5.10 \cdot 10^{-5}$

Tableau III.2.8. Analyses d'incertitudes : résultats[a] pour les analyses de relations

défaut ou défaillance *d*	effet individuel sur la fonction globale *mesurer* i.e. $P[DG_{d,1}]$		effet individuel sur la fonction globale *diagnostiquer* i.e. $P[DG_{d,2}]$	
	espérance i.e. $E[P[DG_{d,1}]]$	variance i.e. $V[P[DG_{d,1}]]$	espérance i.e. $E[P[DG_{d,2}]]$	variance i.e. $V[P[DG_{d,2}]]$
1	*0.990*	$4.96 \cdot 10^{-5}$	*0.930*	$9.79 \cdot 10^{-4}$
2	*1.000*	$3.62 \cdot 10^{-8}$	*0.998*	$2.00 \cdot 10^{-6}$
3	*0.896*	$2.26 \cdot 10^{-3}$	*0.737*	$4.95 \cdot 10^{-3}$
4	*0.708*	$5.62 \cdot 10^{-3}$	*0.674*	$6.57 \cdot 10^{-3}$
5	*0.965*	$3.34 \cdot 10^{-4}$	*0.897*	$1.43 \cdot 10^{-3}$
6	*0.427*	$6.75 \cdot 10^{-3}$	*0.213*	$3.59 \cdot 10^{-3}$
7	*0.668*	$4.80 \cdot 10^{-3}$	*0.412*	$5.26 \cdot 10^{-3}$
8	*0.879*	$2.17 \cdot 10^{-3}$	*0.786*	$4.72 \cdot 10^{-3}$
9	*0.996*	$7.88 \cdot 10^{-6}$	*0.989*	$4.14 \cdot 10^{-5}$

[a]Ces résultats ont été obtenus d'après *10 000* de simulations de Monte Carlo pour chaque ligne, en utilisant les données du Tableau III.2.5.

Tableau III.2.9. Analyses d'incertitudes : résultats[a] pour les probabilités de dysfonctionnements

cas	incertitudes considérées	probabilités de dysfonctionnements de la fonction globale *mesurer* au temps $t = 60$ jours i.e. $P[G_1](60$ jours$)$	
		espérance i.e. $E[P[G_1](60$ jours$)]$	variance i.e. $V[P[G_1](60$ jours$)]$
.	aucune[b]	$4.31 \cdot 10^{-3}$	-
cas i	dans les relations uniquement[c]	$4.39 \cdot 10^{-3}$	$9.66 \cdot 10^{-8}$
cas ii	dans les défauts et défaillances uniquement[d]	$4.31 \cdot 10^{-3}$	$7.72 \cdot 10^{-6}$
cas iii	dans les relations et les défauts et défaillances[e]	$4.37 \cdot 10^{-3}$	$8.47 \cdot 10^{-6}$

cas	incertitudes considérées	probabilités de dysfonctionnements de la fonction globale *diagnostiquer* au temps $t = 60$ jours i.e. $P[G_2](60$ jours$)$	
		espérance i.e. $E[P[G_2](60$ jours$)]$	variance i.e. $V[P[G_2](60$ jours$)]$
.	aucune[b]	$2.38 \cdot 10^{-3}$	-
cas i	dans les relations uniquement[c]	$3.15 \cdot 10^{-3}$	$1.15 \cdot 10^{-7}$
cas ii	dans les défauts et défaillances uniquement[d]	$2.38 \cdot 10^{-3}$	$1.35 \cdot 10^{-6}$
cas iii	dans les relations et les défauts et défaillances[e]	$3.14 \cdot 10^{-3}$	$3.61 \cdot 10^{-6}$

[a]Ces résultats ont été obtenus d'après *100 000* de simulations de Monte Carlo pour chaque ligne.
[b]Les résultats de cette ligne ont été obtenus en utilisant les données des Tableaux III.2.1 et III.2.3.
[c]Les résultats de cette ligne ont été obtenus en utilisant les données des Tableaux III.2.5 et III.2.3.
[d]Les résultats de cette ligne ont été obtenus en utilisant les données des Tableaux III.2.1 et III.2.6.
[e]Les résultats de cette ligne ont été obtenus en utilisant les données des Tableaux III.2.5 et III.2.6.

plusieurs étoiles sur la Figure III.1.4, sont sans incertitudes (uniquement pour des relations totales ou nulles), et les valeurs d'entrée correspondantes sont donc toujours celles du Tableau III.2.1.

Lorsque que des incertitudes dans les relations sont considérées (cas i et iii), les analyses d'incertitudes peuvent être effectuées sur les valeurs de relations totales, par exemple entre les défauts et défaillances et les fonctions globales, indépendamment des probabilités d'occurrence des défauts et des défaillances, comme dans la Section III.2.2.1. Les propriétés des variables aléatoires $P[DG_{d,1}]$ et $P[DG_{d,2}]$, qui représentent les effets individuels des défauts et défaillances sur les fonctions globales *mesurer* et *diagnostiquer*, sont donnés dans le Tableau III.2.8. Les espérances de ces résultats diffèrent légèrement des résultats obtenus dans la Section III.2.2.1 (cf. Tableau III.2.2) car les espérances des valeurs de relations du Tableau III.2.5 ne sont pas toutes égales aux valeurs de relations du Tableau III.2.1. Les incertitudes, d'après les variances des résultats, sont traduites graphiquement sur la Figure III.1.4, d'après le Tableau III.2.7. On remarque alors que les variances obtenues pour ces résultats sont, au plus, du même ordre de grandeur que les variances des valeurs des relations d'entrée (de l'ordre de 10^{-3}, cf. Tableau III.2.5) et, dans plusieurs cas, les ordres de grandeur sont plus petits, en particulier pour les valeurs « extrêmes » (lorsque l'espérance est proche de *1.000*). Ces caractéristiques tendent à démontrer que l'approche proposée est robuste, c'est-à-dire que même si les données d'entrée sont plutôt incertaines, des résultats d'analyses peuvent être obtenus avec une confiance relativement bonne et, dans bien des cas, même meilleure que celle des données d'entrée. Selon cette approche, les incertitudes dans les relations directes utilisées en entrée ont été en partie mutuellement compensées. Des éléments de démonstration de ces propriétés sont présentés dans la Section III.3.3.2.

Finalement, les analyses d'incertitudes pour les trois cas considérés ont été effectuées sur les probabilités de dysfonctionnements des fonctions globales *mesurer* et *diagnostiquer* au temps $t = 60$ jours, d'après *100 000* simulations de Monte Carlo pour chacun des cas (ces analyses pourraient également être effectuées sur les probabilités de mode de défaillance). Ces résultats sont donnés dans le Tableau III.2.9. À titre de comparaison, les résultats obtenus dans la Section III.2.2.2 (sans incertitude) ont également été reportés. Les espérances sont logiquement très proches les unes des autres, mais diffèrent légèrement lorsque des incertitudes sont considérées dans les relations, pour les même raisons qu'expliquées précédemment. D'après les variances, on remarque que la plus grande part d'incertitude dans les résultats a pour origine les incertitudes dans les défauts et défaillances, bien que les incertitudes dans les données d'entrée soient plus grandes pour les relations que pour les défauts et les défaillances (cf. Tableaux III.2.5 et III.2.6). En utilisant l'approche proposée, lorsque les incertitudes dans les taux de défaillance sont prises en compte, l'ajout des incertitudes liées aux comportements du système (par l'intermédiaire des relations entre éléments) n'implique donc pas de fortes incertitudes supplémentaires dans les résultats.

III.2.3. Conclusions Partielles et Perspectives

Afin de prendre en compte les particularités des CTI, une modélisation « 3-Step » est proposée, qui représente les fonctions du système par un arbre des fonctions, ses éléments matériels par un arbre des éléments matériels, et inclut les défauts et défaillances dans une troisième partie. Le comportement du système est ensuite représenté par des matrices de relations qui expriment les probabilités que chaque évènement de défectuosité implique directement un état défaillant ou un dysfonctionnement des autres éléments (éléments matériels et fonctions). Tout d'abord, les analyses de relations permettent notamment d'évaluer les effets de n'importe quel défaut ou défaillance sur les fonctions du système, dans une approche probabiliste. Ensuite, les probabilités de dysfonctionnements et de modes de défaillance sont évaluées en fonction du temps, en prenant en

compte les relations totales entre les éléments du système. Les modes de défaillance sont également définis et évalués d'après la capacité du système à réaliser ses fonctions principales. Enfin, des analyses d'incertitudes ont montré que ces résultats sont robustes, même si les taux de défaillance et les comportements du système (par l'intermédiaire des relations entre éléments) sont mal connus.

Le modèle proposé et les analyses de fiabilité associées sont donc particulièrement adaptés aux CTI et, d'une manière générale, aux systèmes qui présentent de nombreuses interactions internes entre éléments matériels et/ou fonctions, et/ou des comportements mal connus, et ce, même si le retour d'expérience est faible. Pour l'exemple des CTI, la pertinence des fonctionnalités numériques au sein de capteurs-transmetteurs peut alors être appréciée au regard de la fiabilité. En phase de conception, des paramètres comme, par exemple, des facteurs d'importance pour les éléments matériels, et des couvertures de défauts et défaillances pour les fonctions, peuvent être définis avec l'aide de l'approche proposée. Les modes opérationnels des systèmes de contrôle-commande intégrant des CTI peuvent aussi tirer avantage de telles analyses, par exemple en prenant en compte les probabilités de dysfonctionnements et de modes de défaillance pour définir les règles de décision.

À partir de cette première approche du modèle « 3-Step », plusieurs perspectives de développement sont envisageables afin de représenter de façon plus adéquate les particularités de certains systèmes. Notamment, des niveaux additionnels de décomposition des fonctions du système et de ses éléments matériels peuvent être introduits, ainsi que différentes portes logiques pour représenter les relations entre éléments (défauts et défaillances, éléments matériels, fonctions). Ces deux extensions du modèle « 3-Step » sont développées dans la Section III.3, ainsi que les analyses de fiabilité associées, et en particulier les analyses d'incertitudes.

III.3. EXTENSION DU MODÈLE ET DES ANALYSES D'INCERTITUDES

III.3.1. Introduction de Portes Logiques « Continues » pour Arbres de Défaillance

III.3.1.1. Complément à la définition des relations

D'après la définition des relations présentées dans la Section III.2.1.1 (et notamment les Équations III.2.1 à III.2.5), l'état défaillant ou le dysfonctionnement d'un élément amont (élément matériel ou fonction) se produit si un évènement de défectuosité relatif à un élément aval (défaut ou défaillance, élément matériel, ou fonction) se produit, et que l'*évènement de relations directes* entre ces deux éléments se produit (cf. arbres de défaillance équivalents décrits sur la Figure III.2.1). Cette définition des relations est maintenant complétée par l'ajout d'une combinaison supplémentaire d'évènements impliquant l'occurrence de ces évènements de défectuosité (évènements sommet) : si tous les évènements de défectuosité relatifs aux éléments aval (et dont la relation avec l'élément amont n'est pas nulle) se produisent, alors l'évènement de défectuosité de l'élément amont se produit, quels que soit les évènements de relations directes.

L'occurrence de l'évènement de défectuosité de l'élément amont (évènement sommet) dû à l'occurrence de l'ensemble des évènements de défectuosité des éléments aval (évènements basiques) est qualifiée d' « *évènement de relations logiques* ». En effet, ce complément au modèle correspond à une conjoncture intuitive où, par exemple, lorsque que tous les éléments matériels qui ont été identifiés comme intervenant dans la réalisation d'une fonction sont dans des états défaillants, alors, en toute logique, la fonction en question dysfonctionne nécessairement, quelque soit les effets individuel de chacun des éléments matériels. Le modèle intégrant ainsi ce type de relation est donc plus rigoureusement défini. Notons cependant que, dans de nombreux cas (lorsqu'un certain nombre d'éléments aval ont été identifiés pour chaque élément amont, et que qu'un certain nombre de relations directes correspondantes sont assez fortes), les contributions des évènements de relations logiques sont souvent négligeables face à celles des évènements de relations directes, pour l'évaluation de la fiabilité d'un système.

Afin de formaliser ces notions, une porte logique dite de type « *continue* » est introduite dans la section suivante. Cette porte exprime (de façon compacte) à la fois les relations directes et les relations logiques, en utilisant les probabilités d'occurrence des évènements de relations directes comme « *poids* » (paramètres). Les propriétés de cette porte (justifiant notamment le qualificatif de « continue ») sont également présentées dans la section suivante.

III.3.1.2. Porte logique « continue » et propriétés

Une *porte logique « continue »* (ou « C ») est représentée sur la Figure III.3.1. Celle-ci est donnée avec N évènements basiques E_i, associés respectivement aux poids p_i (figurant dans des cercles situés au dessus des évènements basiques), et $0 \leq p_i \leq 1$ (ces poids p_i correspondent, en fait, aux probabilités d'évènements de relations directes). L'évènement sommet d'une porte « continue » se produit alors si au minimum l'une de ces conditions est remplie :

i. n'importe quel évènement basique E_i se produit et implique, avec une probabilité égale à p_i, l'occurrence de l'évènement sommet (relations directes) ; ou
ii. tous les évènements basiques E_i se produisent (relations logiques).

En introduisant des évènements fictifs P_i, dont les probabilités d'occurrence sont respectivement égales aux poids p_i, une porte « continue » est équivalente à l'arbre de défaillance décrit sur la Figure III.3.2. En faisant l'hypothèse que les évènements E_i et P_i sont indépendants, et en notant $P[E_i](t)$ la probabilité que l'évènement E_i se produise avant l'instant t puis reste dans cet état, alors la probabilité que l'évènement sommet d'une porte « continue » se produise avant l'instant t, notée $P[\text{sommet}](t)$, est (cf. preuve en Annexe, Section VI.2.1) :

$$P[\text{sommet}](t) = 1 - \prod_{i=1,\dots,N} (1 - p_i \cdot P[E_i](t)) + \prod_{i=1,\dots,N} ((1 - p_i) \cdot P[E_i](t)) \qquad \text{[III.3.1]}$$

Dans l'Équation III.3.1, la contribution de la condition i est exprimée par $1 - \prod_{i=1,\dots,N} (1 - p_i \cdot P[E_i](t))$, tandis que celle de la condition ii est exprimée par $\prod_{i=1,\dots,N} ((1 - p_i) \cdot P[E_i](t))$. Lorsqu'un certain nombre d'évènements basiques E_i est considéré, et qu'un certain nombre de poids p_i ont une valeur proche de *1.000*, alors la contribution de la condition ii peut souvent être jugée négligeable face à celle de la condition i.

Des exemples de fonctions de défiabilité définies par l'Équation III.3.1 sont représentés sur la Figure III.3.3, avec $N = 3$, $P[E_i] = 1 - exp(-0.001 \cdot t)$ pour $i = 1, \dots, N$, et les poids p_i donnés dans le Tableau III.3.1. Lorsque tous les poids sont égaux à *0.000*, une porte « continue » est équivalente à une porte « et » (c'est-à-dire qui correspond à une structure en parallèle), et lorsque tous les poids sont égaux à *1.000*, une porte « continue » est équivalente à une porte « ou » (c'est-à-dire qui correspond à une structure en série). De plus, la fiabilité de tout système cohérent est comprise entre une fonction de fiabilité correspondant à une structure parallèle (pour le cas le plus fiable) et à une structure série (pour le cas le moins fiable) [RBa75, MRa02]. En agissant sur les valeurs de ses poids, une porte « continue » permet donc une paramétrisation de nature continue (les poids sont des réels) des relations entre les éléments d'un système (d'où son appellation de porte « continue »).

III.3.2. Extension du Modèle « 3-Step »

III.3.2.1. Modèle « 3-Step » étendu avec des portes logiques « continues »

En accord avec la définition des relations présentées dans la Section III.2.1.1, et le complément à cette définition présenté dans la Section III.3.1.1, les relations entre un élément amont et ses éléments aval au sein du modèle « 3-Step » peuvent être représentées par des portes logiques « continues » dont les poids prennent les valeurs des relations directes. Dans l'approche utilisée dans la Section III.2, seuls les évènements de relations directes (cf. condition i de la Section III.3.1.2, et Figure III.3.2, ainsi que la comparaison avec la Figure III.2.1) étaient pris en compte. Dans la présente section, les évènements de relations logiques (cf. condition ii de la Section III.3.1.2, et Figure III.3.2) sont ajoutés. Lorsque des relations entre éléments du système (défauts et défaillances, éléments matériels, fonctions) sont indéfinies (les relations de cause à effet entre évènements de défectuosité ne sont pas « certaines » et doivent ainsi être paramétrés par des probabilités), des portes « continues » peuvent alors être utilisées. Ces incertitudes de modèles sont souvent due à la complexité des systèmes, telles que définies par la norme CEI 61508 [IEC10] : les modes de défaillance de certains composants ne sont pas bien définis ; et/ou des comportements du système en cas de défauts ou de défaillances ne peuvent pas être complètement définis (le système

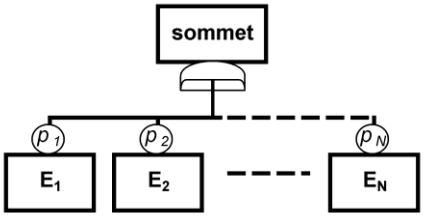

Figure III.3.1. Porte logique « continue » pour arbre de défaillance

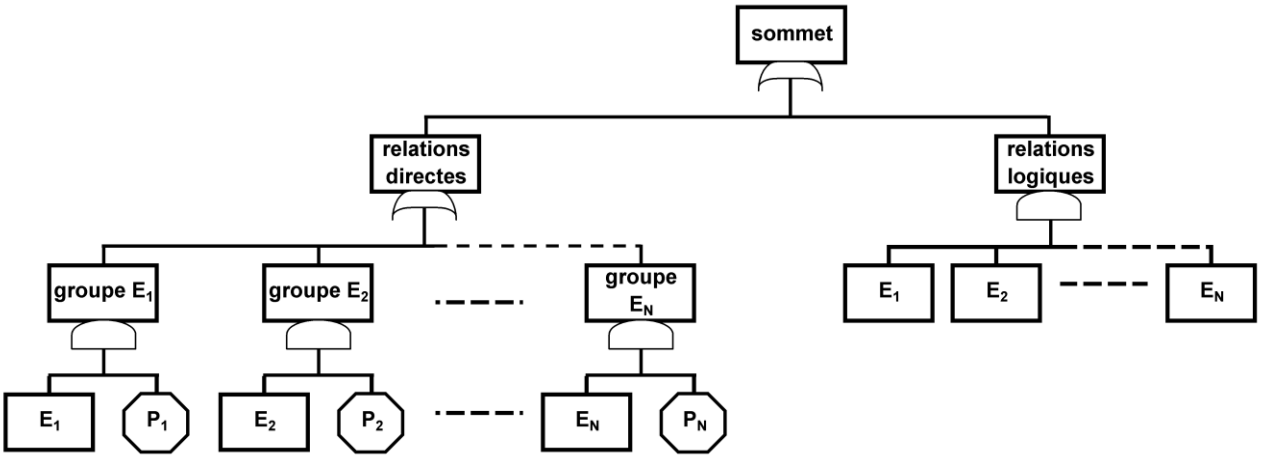

Figure III.3.2. Arbre de défaillance équivalent à une porte logique « continue »

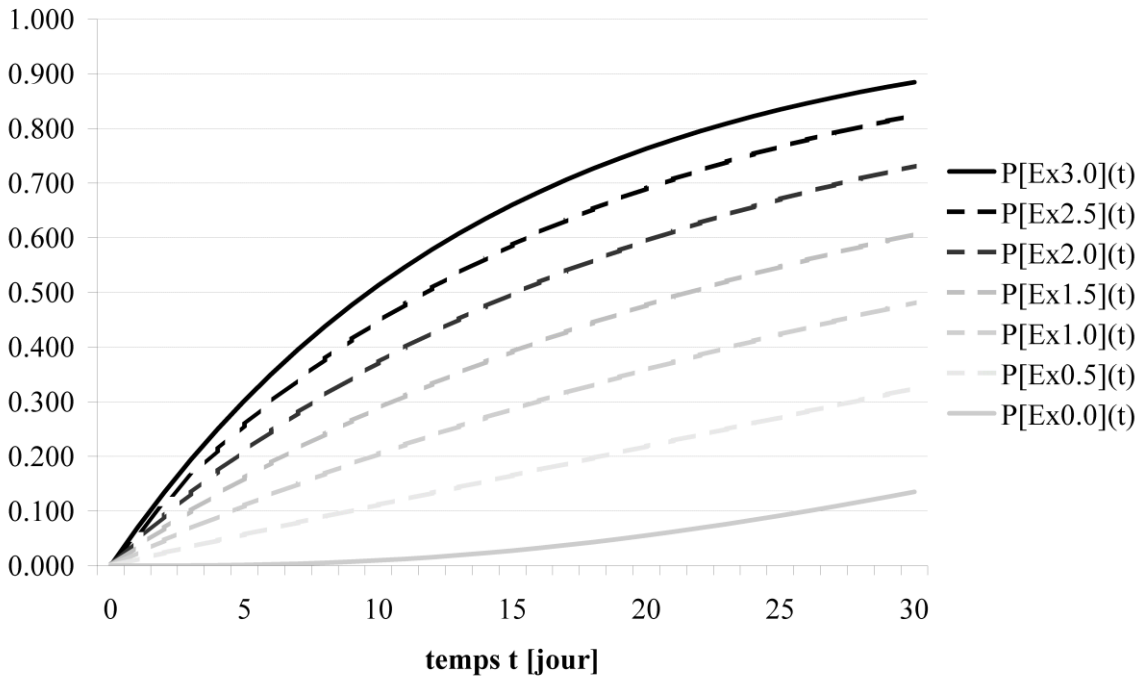

Figure III.3.3. Fonctions de défiabilité d'une porte logique « continue » : illustrations (cf. Section III.3.1.2 et Tableau III.3.1)

Tableau III.3.1. Fonctions de défiabilité d'une porte logique « continue » : exemples

poids			fonctions de défiabilité
p_1	p_2	p_3	
0.000	*0.000*	*0.000*	$P[Ex_{0.0}](t)$[a]
0.500	*0.000*	*0.000*	$P[Ex_{0.5}](t)$
0.500	*0.500*	*0.000*	$P[Ex_{1.0}](t)$
0.500	*0.500*	*0.500*	$P[Ex_{1.5}](t)$
1.000	*0.500*	*0.500*	$P[Ex_{2.0}](t)$
1.000	*1.000*	*0.500*	$P[Ex_{2.5}](t)$
1.000	*1.000*	*1.000*	$P[Ex_{3.0}](t)$[b]

[a]Fonction équivalente à celle d'une structure en parallèle, c'est-à-dire d'une porte logique « et »
[b]Fonction équivalente à celle d'une structure en série, c'est-à-dire d'une porte logique « ou »

est alors qualifié de « type B » d'après cette norme, cf. Section I.2.2.3). (Dans la suite, des analyses d'incertitudes sur les poids des portes « continues » permettront de tester la robustesse des résultats face à ces incertitudes). Dans l'extension proposée du modèle « 3-Step », des portes « et » et « ou » sont également utilisées (ces portes peuvent être définies comme des cas particuliers des portes « continues », cf. Section III.3.1.2). Ces deux dernières sont alors utilisées pour définir des relations connues entre éléments, tout comme dans un arbre de défaillance classique. Enfin, une plus grande flexibilité du modèle est également proposée en intégrant des niveaux de détail supplémentaires dans la décomposition du système (arbres des éléments matériels et des fonctions).

Le modèle « 3-Step » étendu avec des portes logiques « continues », « et », et « ou », est appliqué à un extrait du cas d'étude présenté dans les Section III.1.3 et III.2.2, et est décrit sur la Figure III.3.4. (Les portes logiques étant définies pour représenter des relations de cause à effet entre des évènements de défectuosité, celles-ci sont orientées « défaillance », tout comme pour les arbres de défaillance, et contrairement à la construction des arbres des éléments matériels et des fonctions.) Afin de rendre l'exemple plus didactique, une seule fonction globale (*mesurer*) a été considérée. De plus, les relations entre la fonction globale et les fonctions de base ne sont plus données par une porte « et », mais sont représentées par une porte « continue » qui prend alors mieux en compte les relations indéterminées entre ces fonctions. De par l'utilisation des portes « continues » qui intègrent maintenant, en plus, les évènements de relations logiques (cf. condition ii dans la Section III.3.1.2), certaines valeurs de relations peuvent être définies comme étant un peu plus faibles, c'est ici le cas des relations entre l'élément matériel *carte numérique* et les fonctions de support et de base (cela permet alors de mieux prendre en compte les possibilités d'états défaillants de la *carte numérique* qui n'impliquent que les dysfonctionnements de certaines fonctions). N'ayant maintenant qu'une unique fonction globale, les relations de l'élément matériel *carte numérique* avec les autres éléments du système sont simplement modélisées par l'intermédiaire des fonctions, et non dans des parties inférieures du modèle (par exemple, par les relations entre les défauts et défaillances et les éléments matériels). Dans un souci de clarification du modèle, les arbres des éléments matériels et des fonctions ne sont pas représentés, mais uniquement les éléments des derniers niveaux (les analyses conduisant à l'identification de ces éléments ayant été effectuées précédemment). Pour la même raison, les éléments matériels de support ne sont pas pris en compte dans cet exemple (ainsi que les défauts et défaillances associés), car leurs effets individuels sur les fonctions du système sont assez évidents (cf. résultats des analyses de relations obtenus dans les Sections III.2.2.1 et III.2.2.3). En revanche, des niveaux supplémentaires d'éléments matériels ont été intégrés afin de détailler certains éléments du système (les *éléments de chauffage des optiques*), et de modéliser directement certaines structures internes (celles de l'unité de base *capteurs de température*, cf. Section III.2.2.2), ce qui est maintenant permis par l'utilisation de différentes portes logiques. Tirant profit de ce niveau de détail supplémentaire, des défaillances de cause commune ont également été ajoutées (*défaut ou défaillance des thermistances*).

III.3.2.2. Analyses par arbre de défaillance

Afin d'effectuer les analyses de fiabilité, le modèle « 3-Step » de la Figure III.3.4 a été traduit en arbre de défaillance équivalent qui, grâce à la représentation « compacte » permise par les portes « continues », est décrit sur la Figure III.3.5. Les identifiants des évènements de défectuosité (évènements représentés sur la Figure III.3.5) sont donnés dans les rectangles situés au dessous de la description de chaque défaut ou défaillance, éléments matériels, et fonctions. D'après la définition des portes « continues », les évènements de relations directes ne sont pas explicitement représentés en tant qu'évènements sur la Figure III.3.5, mais le sont par l'intermédiaire des poids

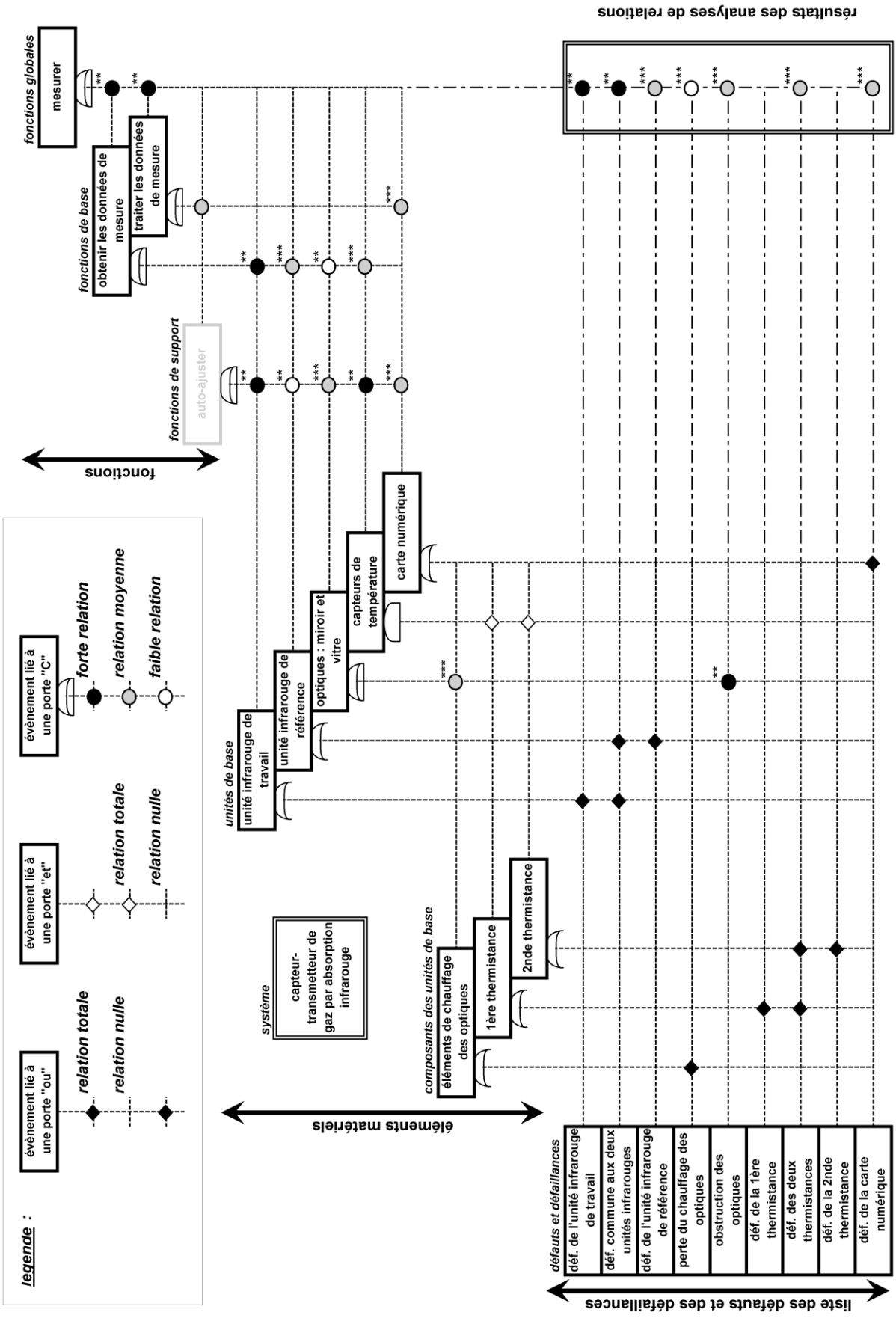

Figure III.3.4. Modèle « 3-Step » étendu avec des portes logiques « continues » (portes « C »)

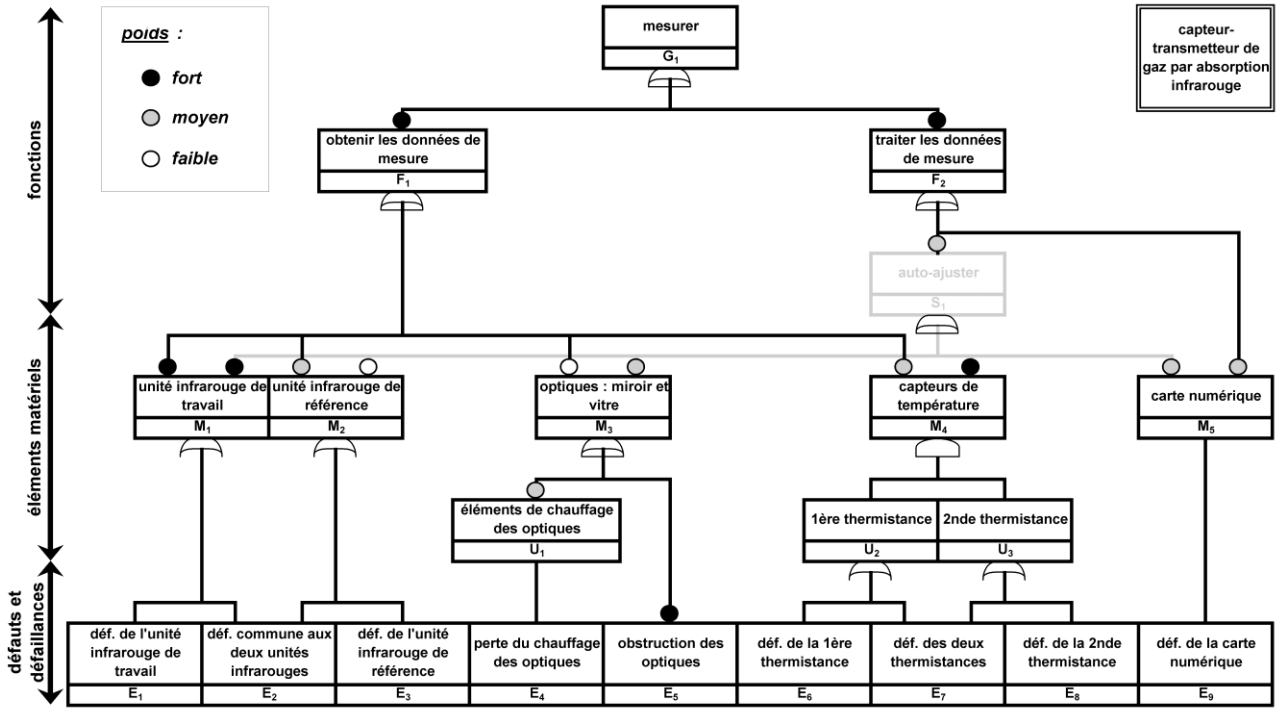

Figure III.3.5. Modèle « 3-Step » étendu représenté sous la forme d'un arbre de défaillance avec des portes logiques « continues »

Tableau III.3.2. Analyses par arbre de défaillance : données d'entrée pour les poids

poids	valeur de base	traduction des résultats pour représentation graphique	analyses d'incertitudes		
			distribution[a,b]	espérance	variance
fort	*0.900*	*0.800* à *1.000*	U[*0.800* ; *1.000*]	*0.900*	$3.33 \cdot 10^{-3}$
moyen	*0.500*	*0.200* à *0.800*	U[*0.200* ; *0.800*]	*0.500*	$3.00 \cdot 10^{-2}$
faible	*0.100*	*0.000* à *0.200*	U[*0.000* ; *0.200*]	*0.100*	$3.33 \cdot 10^{-3}$

[a]U[*a* ; *b*] est une loi Uniforme continue entre la valeur *a* et la valeur *b*.
[b]Plus un poids est défini comme « extrême » (fort ou faible), plus l'incertitude est considérée comme faible, d'après les variances

des portes « continues », situés au dessus des évènements de défectuosité concernés. Suivant les notations présentée dans la Section III.2.1.1, et le formalisme des portes « continues » présenté dans la Section III.3.1.2, l'évènement de relation directe entre l'élément aval *a* (dont l'évènement de défectuosité correspondant est noté A_a et est représenté sur la Figure III.3.5) et l'élément amont *b* (dont l'évènement de défectuosité correspondant est noté B_b et est représenté sur la Figure III.3.5 en tant que parent de l'évènement A_a) est noté $AB_{a,b}$. La probabilité d'occurrence (valeur de relation directe, et qui correspond également à la valeur du poids) de cet évènement est notée $P[AB_{a,b}]$, et est défini par le type (fort, moyen, ou faible) du poids situé au dessus de l'évènement A_a sur la Figure III.3.5.

Les valeurs des poids des portes « continues » (qui correspondent aux valeurs de relations directes) sont définies dans le Tableau III.3.2 (colonne « valeur de base »), d'après leurs types décrits sur la Figure III.3.5 (par l'intermédiaire des couleurs des cercles correspondants). Par exemple, le poids situé au dessus de l'évènement S_1 (dysfonctionnement de la fonction de support *auto-ajuster*) lié à la porte « continue » de l'évènement F_2 (dysfonctionnement de la fonction de base *traiter les données de mesure*), est un poids moyen (qui correspond à l'évènement de relations directes $SF_{1,2}$), donc $P[SF_{1,2}] = 0.500$. (Les données d'entrée du Tableau III.3.2 diffèrent de celles des relations directes utilisées dans la Section III.2.2, cf. Tableau III.2.1, afin d'éviter l'utilisation de poids égaux à *0.000* ou à *1.000* qui, de par l'utilisation des portes « continues », correspondraient directement à des portes « et » et « ou »).

Les défauts et défaillances identifiés dans le modèle « 3-Step » de la Figure III.3.4 sont les évènements basiques de l'arbre de défaillance de la Figure III.3.5. Comme ces défauts et défaillances ne correspondent pas complètement à ceux définis dans les Sections III.1.3 et III.2.2 (de par l'omission de celles relatives aux éléments matériels de support et à l'ajout de celles relatives au niveau supplémentaire de la décomposition du système, cf. Section III.3.2.1), d'autres identifiants ont été choisis afin d'éviter les confusions. Ainsi, l'évènement E_e correspond à l'occurrence du défaut ou de la défaillance *e*, avec $e = 1, \ldots, n_e$ et, pour cet exemple, $n_e = 9$ (dans la Section II.2, les notations D_d, *d*, et n_d avaient respectivement été utilisées pour cette définition). La probabilité d'occurrence du défaut ou de la défaillance *e* (évènement basique E_e) au temps *t* est alors notée $P[E_e](t)$, avec $e = 1, \ldots, n_e$, et est définie par $P[E_e](t) = 1 - exp(-\lambda_e \cdot t)$ dont les taux de défaillance λ_e sont données dans le Tableau III.3.3 (colonne « valeur de base »). À titre d'information, les valeurs de $P[E_e](12$ mois$)$ sont données dans le Tableau III.3.4 (colonne « valeur de base »).

Les analyses par arbre de défaillance ont alors été effectuées en utilisant des arbres de défaillance équivalents aux portes « continues » (cf. Figure III.3.2), et SimTree, le module d'Aralia Workshop [Ara09, YDu97a]. Rappelons que l'évènement sommet considéré est le dysfonctionnement de la fonction globale *mesurer*, noté G_1, et la probabilité de cet évènement au temps *t* est donc noté $P[G_1](t)$. Les résultats en termes de coupes minimales (ensembles minimaux d'évènements correspondants aux occurrences des défauts et défaillances et ceux correspondants aux poids, dont l'occurrence assure que l'évènement sommet se produit) sont donnés dans le Tableau III.3.5. Indépendamment des probabilités d'occurrences des défauts et défaillances au temps *t*, des analyses de relations peuvent être effectuées, de la même façon que dans la Section II.2, en utilisant l'Équation III.2.6 (en remplaçant les évènements D_d par E_e et $DG_{d,g}$ par $EG_{e,g}$). Les effets individuels des défauts et défaillances *e* sur la fonction globale *mesurer*, c'est-à-dire $P[EG_{e,1}]$, sont données dans le Tableau III.3.6 (colonne « valeur de base »), et traduits graphiquement sur la Figure III.3.4 (« résultats des analyses de relations »), d'après le Tableau III.3.2 (colonne « traduction des résultats pour représentation graphique »). (De par la redondance des *thermistances*, on constate logiquement que $P[EG_{e,1}]$ est nulle pour $e = 6$ et $e = 8$).

Tableau III.3.3. Analyses par arbre de défaillance : données d'entrée pour les taux de défaillances

taux de défaillance i.e. λ_e	valeur de base [heure^{-1}]	analyses d'incertitudes		
		distribution[a]	espérance [heure^{-1}]	variance [heure^{-2}]
λ_1	$4.00 \cdot 10^{-7}$	Log-Normal	$4.00 \cdot 10^{-7}$	$3.17 \cdot 10^{-14}$
λ_2	$1.00 \cdot 10^{-7}$	Log-Normal	$1.00 \cdot 10^{-7}$	$1.98 \cdot 10^{-15}$
λ_3	$4.00 \cdot 10^{-7}$	Log-Normal	$4.00 \cdot 10^{-7}$	$3.17 \cdot 10^{-14}$
λ_4	$1.00 \cdot 10^{-6}$	Log-Normal	$1.00 \cdot 10^{-6}$	$1.98 \cdot 10^{-13}$
λ_5	$3.00 \cdot 10^{-6}$	Log-Normal	$3.00 \cdot 10^{-6}$	$1.78 \cdot 10^{-12}$
λ_6	$5.00 \cdot 10^{-7}$	Log-Normal	$5.00 \cdot 10^{-7}$	$4.95 \cdot 10^{-14}$
λ_7	$1.50 \cdot 10^{-7}$	Log-Normal	$1.50 \cdot 10^{-7}$	$4.45 \cdot 10^{-15}$
λ_8	$5.00 \cdot 10^{-7}$	Log-Normal	$5.00 \cdot 10^{-7}$	$4.95 \cdot 10^{-14}$
λ_9	$5.00 \cdot 10^{-7}$	Log-Normal	$5.00 \cdot 10^{-7}$	$4.95 \cdot 10^{-14}$

[a]Les paramètres des lois Log-Normales ont été définis de telle sorte que les moyennes soient égales aux valeurs de base et les facteurs d'erreur soient égaux à *5*.

Tableau III.3.4. Analyses par arbre de défaillance : données d'entrée pour les évènements basiques (occurrence des défauts et défaillances)

évènement basique (occurrence du défaut ou de la défaillance *e*) i.e. E_e	probabilité d'occurrence de l'évènement basique E_e au temps $t = 12$ mois i.e. $P[E_e](12 \text{ mois})$		
	valeur de base[a] i.e. $P[E_e](12 \text{ mois})$	analyses d'incertitudes[b]	
		espérance i.e. $E[P[E_e](12 \text{ mois})]$	variance i.e. $V[P[E_e](12 \text{ mois})]$
E_1	$3.50 \cdot 10^{-3}$	$3.50 \cdot 10^{-3}$	$1.17 \cdot 10^{-5}$
E_2	$8.76 \cdot 10^{-4}$	$8.76 \cdot 10^{-4}$	$7.35 \cdot 10^{-7}$
E_3	$3.50 \cdot 10^{-3}$	$3.50 \cdot 10^{-3}$	$1.17 \cdot 10^{-5}$
E_4	$8.72 \cdot 10^{-3}$	$8.68 \cdot 10^{-3}$	$6.99 \cdot 10^{-5}$
E_5	$2.52 \cdot 10^{-2}$	$2.56 \cdot 10^{-2}$	$5.74 \cdot 10^{-4}$
E_6	$4.37 \cdot 10^{-3}$	$4.36 \cdot 10^{-3}$	$1.80 \cdot 10^{-5}$
E_7	$1.31 \cdot 10^{-3}$	$1.31 \cdot 10^{-3}$	$1.63 \cdot 10^{-6}$
E_8	$4.37 \cdot 10^{-3}$	$4.36 \cdot 10^{-3}$	$1.81 \cdot 10^{-5}$
E_9	$4.37 \cdot 10^{-3}$	$4.36 \cdot 10^{-3}$	$1.80 \cdot 10^{-5}$

[a]Ces résultats ont été obtenus en utilisant l'expression $P[E_e](12 \text{ mois}) = 1 - exp(-\lambda_e \cdot 12 \text{ mois})$, lorsque les taux de défaillance λ_e sont égaux aux valeurs de base telles que données dans le Tableau III.3.3 (colonne « valeur de base »).
[b]Ces résultats ont été obtenus d'après *1 000 000* de simulations de Monte Carlo pour chaque ligne, en utilisant l'expression $P[E_e](12 \text{ mois}) = 1 - exp(-\lambda_e \cdot 12 \text{ mois})$, et lorsque les taux de défaillance λ_e suivent des lois Log-Normales telles que données dans le Tableau III.3.3 (colonnes « analyses d'incertitudes »).

Tableau III.3.5. Analyses par arbre de défaillance : résultats pour les coupes minimales

nombre de coupes minimales	nombre d'évènements basiques E_e dans les coupes minimales	nombre d'évènements correspondants à des poids dans les coupes minimales	probabilités d'occurrence des coupes minimales au temps $t = 12$ mois
25	*1*	*2* à *4*	$2.19 \cdot 10^{-5}$ à $5.23 \cdot 10^{-3}$
66	*2*	*2* à *4*	$1.91 \cdot 10^{-8}$ à $5.95 \cdot 10^{-5}$
70	*3*	*2* à *4*	$1.67 \cdot 10^{-10}$ à $4.45 \cdot 10^{-7}$
51	*4*	*1* à *3*	$3.50 \cdot 10^{-12}$ à $1.56 \cdot 10^{-9}$
27	*5*	*0* à *3*	$5.10 \cdot 10^{-14}$ à $4.91 \cdot 10^{-12}$
9	*6*	*0* à *2*	$2.64 \cdot 10^{-15}$ à $4.76 \cdot 10^{-14}$
1	*7*	*0*	$2.31 \cdot 10^{-16}$

Tableau III.3.6. Analyses par arbre de défaillance : résultats[a] pour les analyses de relations

défaut ou défaillance *e*	effet individuel sur la fonction globale *mesurer* i.e. $P[EG_{e,1}]$		
	valeur de base i.e. $P[EG_{e,1}]$	analyses d'incertitudes[a]	
		espérance i.e. $E[P[EG_{e,1}]]$	variance i.e. $V[P[EG_{e,1}]]$
1	*0.891*	*0.891*	$2.75 \cdot 10^{-3}$
2	*0.919*	*0.919*	$1.85 \cdot 10^{-3}$
3	*0.475*	*0.475*	$2.34 \cdot 10^{-2}$
4	*0.147*	*0.147*	$6.14 \cdot 10^{-3}$
5	*0.265*	*0.265*	$1.05 \cdot 10^{-2}$
6	*0.000*	*0.000*	*0.000*
7	*0.675*	*0.675*	$1.61 \cdot 10^{-2}$
8	*0.000*	*0.000*	*0.000*
9	*0.675*	*0.675*	$1.48 \cdot 10^{-2}$

[a]Ces résultats ont été obtenus d'après *1 000 000* de simulations de Monte Carlo pour chaque ligne, en utilisant les données du Tableau III.3.2 (colonnes « analyses d'incertitudes »).

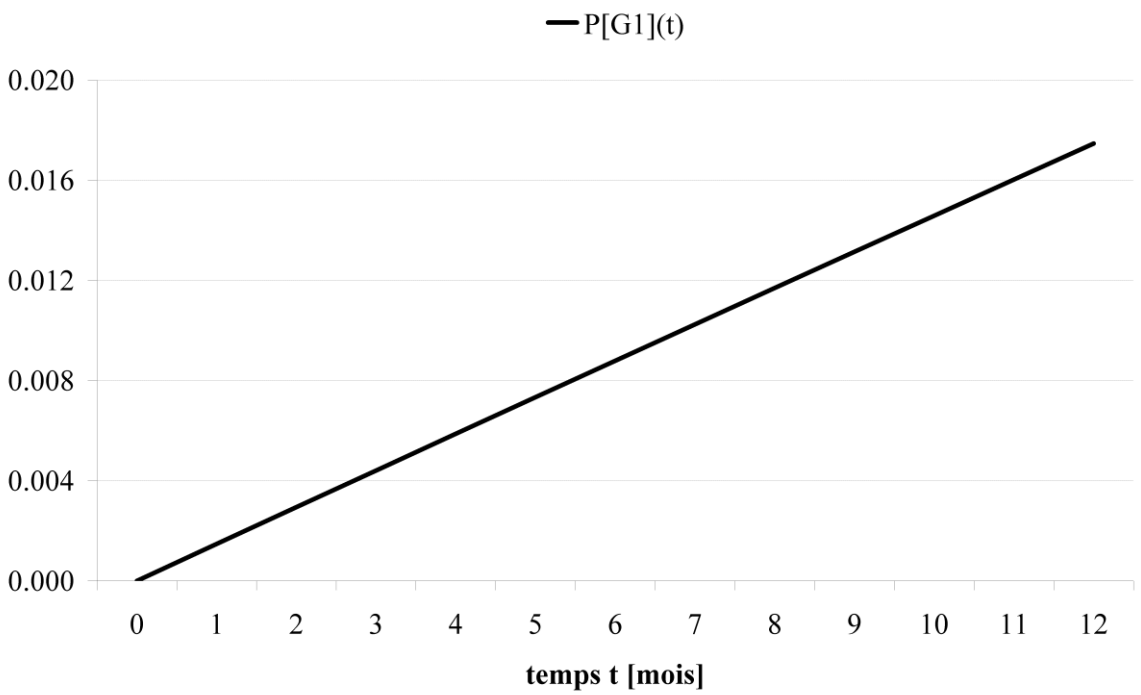

Figure III.3.6. Probabilité de dysfonctionnement de la fonction globale *mesurer* i.e. $P[G_1](t)$

Enfin, en ne considérant aucune action de maintenance sur toute la période d'étude, la probabilité de dysfonctionnement de la fonction globale *mesurer* est représentée sur la Figure III.3.6. Ces derniers résultats sont plus faibles que ceux obtenus dans la Section III.2.2.2, ce qui s'explique notamment par l'omission des défauts ou défaillances des éléments matériels de support (cf. Section III.3.2.1).

III.3.3. Extension des Analyses d'Incertitudes

III.3.3.1. Analyses d'incertitudes à partir du modèle « 3-Step » étendu

Tout comme dans la Section III.2.2.3, trois cas sont considérés afin d'effectuer des analyses d'incertitudes à la fois liées aux paramètres (taux de défaillance) et au modèle (par l'intermédiaire des poids des portes « continues »), et ensuite d'être en mesure d'évaluer les contributions respectives de ces incertitudes d'entrée sur les résultats :

i. incertitudes dans les poids (des portes « continues ») uniquement (incertitudes liées au modèle), c'est-à-dire que les valeurs des poids ne sont plus définies par les valeurs de base, mais sont des variables aléatoires distribuées selon des lois Uniformes telles que définies dans le Tableau III.3.2 (colonnes « analyses d'incertitudes ») ;
ii. incertitudes dans les taux de défaillance uniquement (incertitudes liées aux paramètres), c'est-à-dire que les taux de défaillance ne sont plus définis par les valeurs de base, mais sont des variables aléatoires distribuées selon des lois Log-Normales telles que définies dans le Tableau III.3.3 (colonnes « analyses d'incertitudes ») ;
iii. incertitudes dans les poids et les taux de défaillance (incertitudes liées au modèle et aux paramètres).

À la fois les distributions pour les valeurs des poids et les taux de défaillance ont ici été définies de telle sorte que les espérances soient égales aux valeurs de base. Pour les cas ii et iii, les probabilités d'occurrences des défauts et défaillances au temps t ($P[E_e]t(t)$) sont alors des variables aléatoires, et leurs propriétés (espérances et variances) au temps $t = 12$ mois sont données dans le Tableau III.3.4 (colonnes « analyses d'incertitudes »). À noter que les variances de $P[E_e](12$ mois$)$ sont plus faibles que les variances des valeurs des poids, sur toute la période $[0 ; 12$ mois$]$, c'est-à-dire que, pour les données d'entrée, de plus fortes incertitudes sont considérées pour les poids que pour les évènements basiques (occurrence des défauts et défaillances). Les incertitudes, d'après les variances, sont traduites graphiquement sur la Figure III.3.4, d'après le Tableau III.2.7.

Lorsque des incertitudes dans les poids sont considérées (cas i et iii), les analyses d'incertitudes peuvent être effectuées sur les effets individuels des défauts et défaillances sur la fonction globale *mesurer* ($P[EG_{e,1}]$). Les propriétés des variables aléatoires $P[EG_{e,1}]$ sont données dans le Tableau III.3.6 (colonnes « analyses d'incertitudes »), et les incertitudes correspondantes, d'après les variances, sont traduites graphiquement sur la Figure III.3.4, d'après le Tableau III.2.7.

Les analyses d'incertitudes pour les trois cas considérés ont été effectuées sur la probabilité de dysfonctionnement de la fonction globale *mesurer* au temps $t = 12$ mois ($P[G_1](12$ mois$)$), (les incertitudes dans ce résultat sont croissants au cours du temps de par les incertitudes des évènements basiques), d'après *1 000 000* de simulations de Monte Carlo pour chacun des cas. Ces résultats sont donnés dans le Tableau III.3.7 et les densités de probabilité correspondantes sont représentées sur la Figure III.3.7. On remarque alors que la plus grande part d'incertitude (tout

Tableau III.3.7. Analyses par arbre de défaillance : résultats[a] pour les probabilités de dysfonctionnements

cas	incertitudes considérées	probabilité de dysfonctionnement de la fonction globale *mesurer* au temps *t = 12* mois i.e. *P[*G_1*](12* mois*)*	
		espérance i.e. *E[P[*G_1*](12* mois*)]*	variance i.e. *V[P[*G_1*](12* mois*)]*
.	aucune	$1.75 \cdot 10^{-2}$	-
cas i	dans les poids uniquement (de modèle)	$1.75 \cdot 10^{-2}$	$1.17 \cdot 10^{-5}$
cas ii	dans les taux de défaillance uniquement (de paramètres)	$1.74 \cdot 10^{-2}$	$6.20 \cdot 10^{-5}$
cas iii	dans les poids et les taux les taux de défaillance (de modèle et de paramètres)	$1.74 \cdot 10^{-2}$	$7.97 \cdot 10^{-5}$

[a]Ces résultats ont été obtenus d'après *1 000 000* de simulations de Monte Carlo pour chaque ligne.

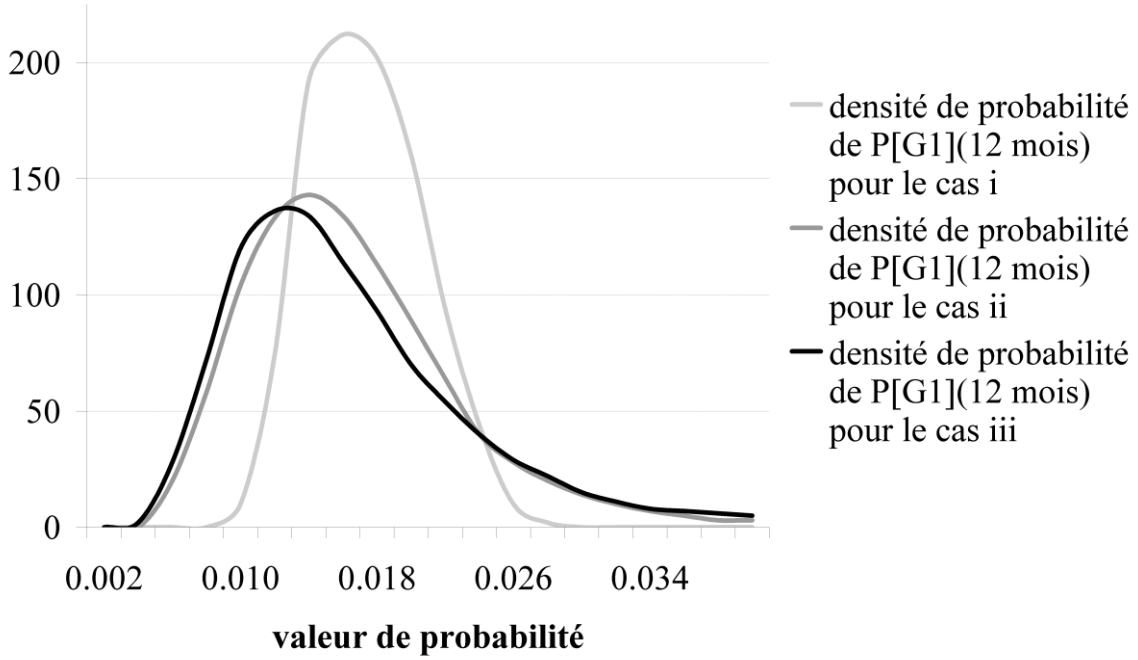

Figure III.3.7. Densités de probabilité (ddp) de la probabilité de dysfonctionnement de la fonction globale *mesurer* au temps *t = 12* mois i.e. *P[*G_1*](12* mois*)*, dans les cas d'analyses d'incertitudes (cf. Tableau III.3.7)

comme pour les analyses effectuées dans la Section III.2.2.3) a pour origine les incertitudes dans les taux de défaillances, bien que les incertitudes dans les données d'entrée soient plus grandes pour les poids que pour les évènements basiques (occurrence des défauts et défaillances), (cf. Tableaux III.3.2 et III.3.4, d'après les variances). De plus, les variances des résultats obtenus pour ces trois cas sont relativement faibles (de l'ordre de 10^{-5}) comparées aux variances des données d'entrée (de l'ordre de 10^{-3} pour les poids, et de 10^{-5} pour la plupart des évènements basiques). Ces propriétés sont discutées dans la section suivante.

III.3.3.2. Discussion des résultats des analyses d'incertitudes

III.3.3.2.1. Discussions préliminaires

Les analyses d'incertitudes ont montré qu'en utilisant l'approche proposée, au moins pour les exemples donnés, les incertitudes à la fois liées au modèle et aux paramètres ne s'opposent pas à l'obtention de résultats relativement « certains ». L'approche proposée est donc robuste et, en particulier, lorsque les incertitudes dans les taux de défaillance sont prises en compte, l'ajout des incertitudes liées aux comportements du système (par l'intermédiaire des poids des portes « continues ») n'implique pas de forte incertitudes supplémentaires dans les résultats (par comparaison des résultats obtenus pour les cas ii et iii). Les incertitudes d'entrée ne se sont donc pas accentuées au travers de l'approche proposée mais, au contraire, en partie mutuellement compensées, et en particulier pour les incertitudes liées au modèle.

À première vue, ces observations peuvent paraître surprenantes. Une première explication intuitive peut, cependant, être apportée. Si l'on considère un ensemble d'évènements indépendants dont l'occurrence de chacun d'eux est très incertaine, il est alors plus raisonnable de prétendre que « au moins l'un de ces évènements se produira », plutôt que « un de ces évènements en particulier se produira » et, de même, « au moins l'un de ces évènements ne se produira pas », plutôt que « un de ces évènements en particulier ne se produira pas ». En traduisant ces assertions en arbres de défaillance, les deux premières peuvent se rapporter à l'occurrence d'un évènement modélisé par une porte « ou », et les deux secondes à la non-occurrence d'un évènement modélisé par une porte « et ». Il est ainsi supposé que la probabilité d'occurrence d'un évènement modélisé par une porte « ou » ou de la non-occurrence d'un évènement modélisé par une porte « et » (et donc l'opposé) peut être évalué avec une plus faible incertitude que celle liées aux occurrences de n'importe quel évènement basique utilisé. Ces propriétés sont démontrées dans la section suivante en utilisant les densités de probabilité et les variances.

III.3.3.2.2. Densités de probabilité et variances

Soient X et Y deux variables aléatoires indépendantes qui décrivent des valeurs de probabilité (dans les cas d'études présentés précédemment, ces variables peuvent être des probabilités d'occurrence d'évènements basiques, ou des poids), dont les densités de probabilités sont respectivement $f_X(x)$ et $f_Y(y)$, donc :

$$\int_0^1 f_X(x) \cdot dx = 1 \qquad \text{et} \qquad f_X(x) \geq 0 \text{ pour } 0 \leq x \leq 1 \qquad \text{[III.3.2]}$$

$$\int_0^1 f_Y(y) \cdot dy = 1 \qquad \text{et} \qquad f_Y(y) \geq 0 \text{ pour } 0 \leq y \leq 1 \qquad \text{[III.3.3]}$$

Il est alors possible d'exprimer la densité de probabilité des variables aléatoires $W = X \cdot Y$ et $Z = 1 - (1 - X) \cdot (1 - Y)$ qui correspondent aux opérations de base utilisées dans les analyses par arbre de défaillance (pour des portes « et » et « ou », respectivement), (cf. preuves en Annexe, Sections VI.2.2 et VI.2.3) :

$$f_W(w) = f_{X \cdot Y}(w) = \int_0^1 f_X(u) \cdot f_Y(w / u) \cdot (1 / u) \cdot du \qquad \text{[III.3.4]}$$

$$f_Z(z) = f_{1-(1-X)\cdot(1-Y)}(z) = \int_0^1 f_X(u) \cdot f_Y((u - z) / (u - 1)) \cdot (1 / (1 - u)) \cdot du \qquad \text{[III.3.5]}$$

De plus, les propriétés suivantes peuvent être établies concernant les espérances et les variances :

$$E[X \cdot Y] = E[X] \cdot E[Y] \qquad \text{[III.3.6]}$$

$$V[X \cdot Y] = V[X] \cdot E^2[Y] + V[Y] \cdot E^2[X] + V[X] \cdot V[Y] \qquad \text{[III.3.7]}$$

$$E[1 - (1 - X) \cdot (1 - Y)] = 1 - (1 - E[X]) \cdot (1 - E[Y]) \qquad \text{[III.3.8]}$$

$$V[1 - (1 - X) \cdot (1 - Y)] = V[X] \cdot (1 - E[Y])^2 + V[Y] \cdot (1 - E[X])^2 + V[X] \cdot V[Y] \qquad \text{[III.3.9]}$$

Les Équations III.3.6 et III.3.8 sont directement obtenues de par les propriétés des espérances, et les Équations III.3.7 et III.3.9 peuvent être facilement démontrées en utilisant la relation $V[X] = E[(X - E[X])^2]$ puis les propriétés des espérances. Enfin, les deux assertions suivantes sont respectivement déduites des Équations III.3.7 et III.3.9 (cf. preuves en Annexe, Section VI.2.4) :

$$\{V[X \cdot Y] \leq min(V[X], V[Y])\} \text{ si et seulement si}$$
$$\{(E^2[X] / V[X]) + (E^2[Y] / V[Y]) \leq (1 / max(V[X], V[Y])) - 1\} \qquad \text{[III.3.10]}$$

$$\{V[1 - (1 - X) \cdot (1 - Y)] \leq min(V[X], V[Y])\} \text{ si et seulement si}$$
$$\{((1 - E[X])^2 / V[X]) + ((1 - E[Y])^2 / V[Y]) \leq 1 / max(V[X], V[Y])\} \qquad \text{[III.3.11]}$$

Les Équations III.3.10 et III.3.11 montrent les conditions nécessaires et suffisantes sur les moments des premier et second ordres de deux variables aléatoires pour que le résultat des opérations correspondantes ait une variance plus petite que n'importe laquelle des deux variables d'entrée. En d'autres termes, le résultat de l'opération $X \cdot Y$ (respectivement $1 - (1 - X) \cdot (1 - Y)$) est moins incertain que n'importe laquelle de ses variables d'entrée (X et Y) si et seulement si le second membre de l'Équation III.3.10 (respectivement III.3.11) est vérifiée. À noter que ces conditions ne sont pas systématiquement remplies. Pour un système modélisé avec un certain nombre d'évènements et de paramètres, comme dans les exemples présentés précédemment, ces conditions ont des chances d'être plus souvent remplies, et la réduction des variances au cours des calculs par arbre de défaillance s'explique alors par ces propriétés.

Parce que de mêmes évènements sont souvent présents dans plusieurs termes des opérations utilisées pour effectuer les analyses par arbre de défaillance, plusieurs variables aléatoires ne sont pas indépendantes et il n'est généralement pas possible d'appliquer directement les Équations III.3.4 à III.3.9 pour évaluer la variance du résultat final (probabilité d'occurrence de l'évènement sommet). Néanmoins, un exemple sur deux coupes minimales extraites du cas d'étude précédent est présenté dans la section suivante afin d'illustrer ces résultats.

III.3.3.2.3. Exemple sur des coupes minimales

À partir des analyses par arbre de défaillance présentées dans la Section III.3.2.2, parmi les coupes minimales de premier ordre selon les évènements basiques E_e (d'après le Tableau III.3.5, l'ordre selon les évènements basiques est beaucoup plus significatif qu'un ordre selon des évènements correspondants à des poids, pour les probabilités d'occurrence des coupes minimales), deux incluent l'évènement E_9 (occurrence du *défaut ou défaillance de la carte numérique*). Ces coupes minimales incluent, de plus, les évènements correspondants à des poids (évènements de relations directes) entre les évènements M_5 (état défaillant de l'unité de base *carte numérique*) et S_1 (dysfonctionnement de la fonction de support *auto-ajuster*), c'est-à-dire $MS_{5,1}$; entre les évènements M_5 et F_2 (dysfonctionnement de la fonction de base *traiter les données de mesure*), c'est-à-dire $MF_{5,2}$; et entre les évènements F_2 et G_1 (dysfonctionnement de la fonction globale *mesurer*), c'est-à-dire $FG_{2,1}$. À noter que lorsqu'à la fois les évènements M_5 et S_1 se produisent, les évènements correspondants à des poids entre les évènements M_5 et F_2, c'est-à-dire $MF_{5,2}$, et entre les évènements S_1 et F_2, c'est-à-dire $SF_{1,2}$, sont sans effet car l'évènement F_2 se produit de par un évènement de relations logiques (cf. condition ii de la Section III.3.1.2). Soient les évènements correspondants à l'occurrence des deux coupes minimales en question :

$$MCS_1 = \{E_9 \cap MS_{5,1} \cap FG_{2,1}\} \quad \text{[III.3.12]}$$

$$MCS_2 = \{E_9 \cap MF_{5,2} \cap FG_{2,1}\} \quad \text{[III.3.13]}$$

Il est alors possible d'exprimer l'évènement d'union des deux évènements précédents :

$$\{MCS_1 \cup MCS_2\} = \{(E_9 \cap MS_{5,1} \cap FG_{2,1}) \cup (E_9 \cap MF_{5,2} \cap FG_{2,1})\} \quad \text{[III.3.14]}$$

$$\{MCS_1 \cup MCS_2\} = \{E_9 \cap (MS_{5,1} \cup MF_{5,2}) \cap FG_{2,1}\} \quad \text{[III.3.15]}$$

La probabilité d'occurrence de la coupe minimale MCS_1 ou MCS_2 au temps $t = 12$ mois est donc :

$$P[MCS_1 \cup MCS_2](12 \text{ mois}) = P[E_9](12 \text{ mois}) \cdot (1 - (1 - P[MS_{5,1}]) \cdot (1 - P[MF_{5,2}])) \cdot P[FG_{2,1}] \quad \text{[III.3.16]}$$

Les résultats (espérances et variances) obtenus lors du calcul de la probabilité d'occurrence définie par l'équation III.3.16 sont donnés pas à pas dans le Tableau III.3.8, et les densités de probabilité des variables résultantes des opérations sur les poids sont également représentées sur la Figure III.3.8. On remarque alors qu'à chaque fois que deux variables aléatoires (probabilité d'occurrence de l'évènement basique E_9, c'est-à-dire $P[E_9](12$ mois$)$, et poids $P[MS_{5,1}]$, $P[MF_{5,2}]$, et $P[FG_{2,1}]$) sont combinées dans une opérations, la variable aléatoire obtenue a une variance plus faible que chacune de ses variables d'entrée, illustrant ainsi la réduction des variances lors des analyses de fiabilité effectuées à partir du modèle proposé.

III.3.4. Conclusions Partielles et Perspectives

Les extensions du modèle « 3-Step » utilisées dans cette Section III.3 (niveaux additionnels de décomposition du système, différentes portes logiques) permettent de rendre la modélisation plus flexible et plus complète. De plus, la définition de portes logiques « continues » apporte un moyen de paramétrer les relations entre évènements, ouvrant alors vers des analyses d'incertitudes à la fois liées aux paramètres et au modèle. Le formalisme de cette approche est en adéquation avec les méthodes communes d'évaluations probabilistes des risques (EPR). Ces extensions impliquent cependant une complexification des analyses, ce qui impose l'utilisation de logiciels appropriés. Il serait alors intéressant de valider cette approche en multipliant et en diversifiant les cas d'étude.

Tableau III.3.8. Résultats obtenus lors le calcul de la probabilité d'occurrence d'un exemple de coupes minimales

variable aléatoire	espérance[a]	variance[a]
$P[MS_{5,1}]$	0.500	$3.00 \cdot 10^{-2}$
$P[MF_{5,2}]$	0.500	$3.00 \cdot 10^{-2}$
$P[FG_{2,1}]$	0.900	$3.33 \cdot 10^{-3}$
$P[E_9](12$ mois$)$	$4.37 \cdot 10^{-3}$	$1.80 \cdot 10^{-5}$
$1 - (1 - P[MS_{5,1}]) \cdot (1 - P[MF_{5,2}])$	0.750	$1.59 \cdot 10^{-2}$
$(1 - (1 - P[MS_{5,1}]) \cdot (1 - P[MF_{5,2}])) \cdot P[FG_{2,1}]$	0.675	$1.48 \cdot 10^{-2}$
$P[E_9](12$ mois$) \cdot (1 - (1 - P[MS_{5,1}]) \cdot (1 - P[MF_{5,2}])) \cdot P[FG_{2,1}]$	$2.95 \cdot 10^{-3}$	$8.76 \cdot 10^{-6}$

[a]Ces résultats ont été obtenus en utilisant les équations III.3.6 à III.3.9.

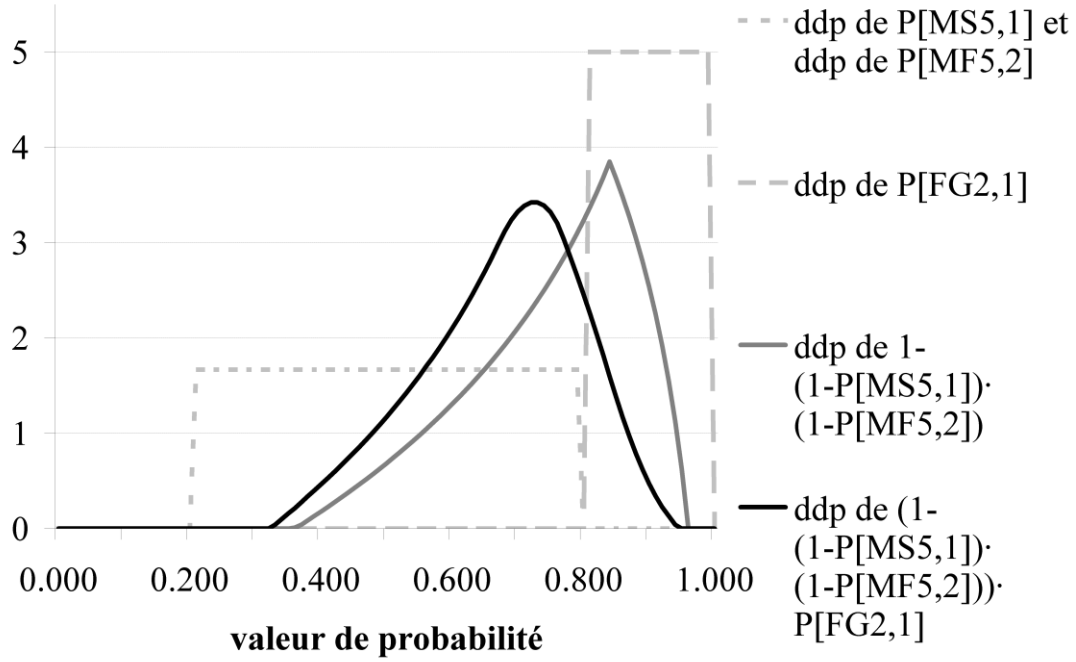

Figure III.3.8. Densités de probabilité (ddp) obtenues lors du calcul de la probabilité d'occurrence d'un exemple de coupes minimales (cf. Tableau III.3.8)

CHAPITRE IV

SYSTÈMES DE CONTRÔLE-COMMANDE INTÉGRANT DES CAPTEURS-TRANSMETTEURS À FONCTIONNALITÉS NUMÉRIQUES

Ce chapitre présente la modélisation et l'évaluation de systèmes de contrôle-commande (SCC) intégrant des « capteurs-transmetteurs intelligents » (CTI). L'enjeu est de proposer une modélisation et une évaluation de ces systèmes qui prenne en compte les interactions entre les CTI puis, dans un second temps, également les interactions avec les autres éléments du système, ainsi qu'avec le processus contrôlé.

La première section de ce chapitre présente les concepts et les problématiques liés à l'utilisation de CTI au sein de SCC. La seconde section introduit un tel système composé de CTI effectuant des opérations en « collaboration ». Enfin, la troisième section développe une approche de fiabilité dynamique afin de prendre en compte à la fois les interactions entre les éléments du système, et en particulier les CTI, et celles avec le processus contrôlé.

La troisième section de ce chapitre, sur la fiabilité dynamique, relate des travaux qui ont été réalisés à l'Université d'État de l'Ohio (OSU), et co-encadrés par Prof. Carol Smidts.

Les publications réalisées en lien avec les travaux de ce chapitre sont présentées dans la Section VII.2.3.

SOMMAIRE DU CHAPITRE IV

IV.1. SYSTÈMES DE CONTRÔLE-COMMANDE ET « CAPTEURS-TRANSMETTEURS INTELLIGENTS »

IV.1.1. Systèmes de Contrôle-Commande à « Intelligence Distribuée »

L'utilisation de capteurs-transmetteurs à « intelligence embarquée » au sein d'un système de contrôle-commande (SCC) permet la « délocalisation » de certaines opérations précédemment effectuées par une unité centrale, vers les éléments du système (capteurs-transmetteurs, contrôleurs, actionneurs, etc.), formant ainsi un *système à « intelligence distribué »* (SID), (ou « *système de contrôle à intelligence distribué* » (SCID), « *système d'automatisation à intelligence distribuée* » (SAID) [JTh04] ; et en anglais, « *distributed control system* » (DCS)). De plus, dans un *système de contrôle en réseau* (SCR), (ou « *système commandé en réseau* » (SCR) ; et en anglais, « *networked control system* » (NCS)), les éléments du SID sont interconnectés par un réseau de communication fonctionnant en temps réel [FWa08]. Les protocoles de réseaux et bus de terrain utilisés pour cela incluent notamment le *Controller area network* (CAN), *Profibus*, *Foundation fieldbus*, et *Device-nets* [YTi03]. Des cas particuliers de SCR sont les réseaux de micro-capteurs sans fil [JYi08, IAk02, FBrPr], mais ces derniers relèvent de problématiques très spécifiques qui sortent du champ d'étude du présent mémoire.

La caractéristique définissant un SCR est que les informations (par exemple, des identifiants, des résultats de mesures, des signaux de contrôle) sont échangées entre les éléments du système (capteurs-transmetteurs, contrôleurs, actionneurs, etc.) via un réseau de communication [BZh01, RGu08], et non par de traditionnelles connections « point à point ». L'utilisation d'un réseau permet également d'effectuer des contrôles et des transferts de données à distance [RGu08, YTi03]. Les SCR offrent alors plusieurs avantages, en particulier une réduction de la complexité des câblages et une diminution des coûts associés, des facilités de maintenance, ainsi qu'une certaine flexibilité, ce qui conduit à une utilisation accrue de ces systèmes dans plusieurs secteurs industriels et notamment dans l'industrie des procédés, l'automobile, et l'aéronautique [RGu08]. Cependant, l'utilisation des SCR induit également certaines problématiques, notamment des délais de communication ainsi que des pertes de données, qui peuvent alors causer certaines instabilités du système et affecter ses performances [JJHe07, BZh01, YGe07, FLi02, YTi03, MBr00]. Les délais sont dus au partage du support de communication, ainsi qu'au temps de calcul requis pour gérer la communication [FLi02, YGe07]. Les pertes de données se produisent lors des transferts de données au sein du réseau, résultant généralement d'erreurs de transmission ou d'une saturation des mémoires tampons [JHe07]. De nombreux travaux de recherche se focalisent alors sur la stabilité des SCR afin de garantir des temps de transmission constants, de minimiser ou de compenser les délais, et d'analyser les effets induits sur les performances du système [BZh01, YGe07, MBr00].

Dans le contexte de la maîtrise des risques technologiques, les critères de performance pertinents sont relatifs à la sûreté de fonctionnement. Une norme sur la sûreté de fonctionnement des réseaux de communication est par ailleurs à l'étude [IEC09]. Les contraintes de sûreté de fonctionnement liées à l'utilisation de bus de communication (problèmes de cohérence temporelle et des caractéristiques du trafic) ont été présentées et discutées dans la littérature [LCa04, LCa03]. Des analyses des modes de défaillance, de leurs effets, et de leurs criticités (AMDEC) correspondantes ont également été proposées [LCa04]. Plusieurs analyses de sûreté de fonctionnement se sont concentrées sur le protocole CAN, par exemple pour étudier les temps de réponse lors de la transmission d'erreurs, en utilisant des approches déterministes [KTi95], ou stochastiques [NNa00],

ou pour étudier les effets d'erreurs [JPe03], en utilisant des techniques d'introduction de défauts. Les interférences électromagnétiques sont les défauts (passagers) les plus souvent pris en compte. En considérant à la fois des défauts passagers et permanents, une évaluation de sûreté de fonctionnement d'un réseau de terrain a également été proposée [PPo04], en utilisant des réseaux de Petri stochastiques. Au regard d'une application, le comportement d'un réseau soumis à des erreurs de transmission a également été modélisé à l'aide des *stochastic activity networks* (SAN), une extension des réseaux de Petri stochastiques, pour évaluer la sûreté de fonctionnement d'un SCR [RGh06, RGh11]. Des analyses quantitatives sont ensuite effectuées par des simulations de Monte Carlo. À noter que ces précédents travaux se sont exclusivement concentrés sur les réseaux de communication, et les défaillances des éléments du SCR tels les capteurs-transmetteurs et les actionneurs n'ont pas été considérés.

Des analyses plus globales de la sûreté de fonctionnement ont pris en compte à la fois le réseau de communication et les éléments du SCR. Par exemple, les scenarios impliquant des défaillances du SCR ont été analysés en considérant des probabilités de perte de données [PBa03]. Pour cela, des réseaux de Petri colorés et stochastiques ont été utilisés, et des analyses ont ensuite été effectuées à l'aide de simulations de Monte Carlo. Cependant, hormis ce qui concerne la communication, les « fonctionnalités intelligentes » des capteurs-transmetteurs et des actionneurs modélisés ne sont pas vraiment prises en compte. Par exemple, seules deux fonctions sont considérées pour un capteur-transmetteur : mesurer et communiquer ; et le seul mode de défaillance est la transmission d'un message d'erreur à la place d'un résultat de mesure, selon une probabilité constante. Des restrictions similaires concernant les caractéristiques des capteurs-transmetteurs et des actionneurs ont été considérées dans d'autres approches d'analyses de sûreté de fonctionnement de SCR [YDa03, BCo05]. À l'inverse, les analyses de fiabilité présentées précédemment dans ce mémoire (cf. Chapitre III) ont été menées sans considération pour les réseaux de communication, et les interactions alors induites entre les éléments d'un SCR n'ont pas été étudiées.

Enfin, des études de sûreté de fonctionnement de SCR (ou SID) peuvent être trouvées dans la littérature au regard des techniques de tolérance aux défauts [NEl05, ZMa07] (en anglais, « *fault tolerant control* » (FTC)). Ces dernières ont pour objectif de maintenir la capacité du système à assurer ses fonctions, malgré la présence de défauts, notamment afin d'améliorer des critères de fiabilité et de sécurité [JCa99], et par exemple sous des contraintes de coûts [NWa01]. De plus, les techniques de détection et d'isolation des défauts [HFa07] (en anglais, « *fault detection and isolation* » (FDI)) cherchent à détecter, isoler, et estimer les défauts, ce qui est souvent requis par les stratégies de tolérance aux défauts. À noter que les réseaux de Petri sont, là aussi, souvent utilisés pour modéliser des SCR (ou SID) tolérants aux défauts, notamment des réseaux de Petri stochastiques [JPi02] ou des SAN [JCa99].

Dans la Section IV.2, les CTI en tant qu'éléments d'un SCR (ou SID) seront étudiés sous un angle de la sûreté de fonctionnement. Des particularités de ces systèmes, autres que celle de communiquer en réseau, seront prises en compte. Ces caractéristiques, rendues possibles par « l'intelligence embarquée », consistent en certaines opérations comme, par exemple, la capacité d'effectuer des traitements de données, des auto-diagnostics, et des reconfigurations en ligne. La contribution de la Section IV.2 peut ainsi être appréciée comme un lien entre les analyses de fiabilité des CTI (cf. Chapitre III), et d'autres travaux sur la sûreté de fonctionnement des SCR [PBa03]. Bien que le cas d'étude présenté dans la Section IV.2 ne prenne pas en compte les performances du réseau de communication, des travaux relatifs à ces aspects [RGh06] peuvent y être facilement intégrés. La communication en temps réel entre les éléments du SCR y est cependant exploitée afin de créer un réseau de capteurs-transmetteurs capable d'améliorer certaines de leurs opérations en s'échangeant des informations. En accord avec la plupart des travaux réalisés sur la sûreté de fonctionnement des

SCR, des approches basées sur les réseaux de Petri seront utilisés. Les réseaux de Petri sont présentés dans la Section IV.1.3. Juste avant cela, la Section IV.1.2 élargit les problématiques de la modélisation des CTI en y intégrant les interactions avec les autres éléments du système, ainsi qu'avec le processus contrôlé, formant alors un problème de fiabilité dynamique. L'application d'une telle approche est finalement présentée dans la Section IV.3, et illustrée par un cas d'étude.

IV.1.2. Interactions du Système avec le Processus Contrôlé – Fiabilité Dynamique

Les approches par arbres d'évènements et de défaillance ont été introduites dans les années soixante-dix [USN75] en se concentrant principalement sur les composants des systèmes et leurs interactions. En particulier, elles ont montré de bonnes capacités pour modéliser des dépendances fonctionnelles entre composants comme, par exemple, l'inclusion des causes communes de défaillance [MSt02]. Cependant, ces approches n'ont pas été conçues pour faire face à des changements de relations entre évènements (dans une séquence ou une combinaison) qui ont lieux au cours du temps, par exemple dus à des interactions avec le processus, l'environnement, ou des opérateurs humains [NSi94]. Elles sont ainsi qualifiées de « statiques ». D'autres modèles « statiques » répandus dans les analyses de fiabilité incluent, par exemple, les diagrammes de fiabilité.

À la fin des années quatre-vingt, et au début des années quatre-vingt-dix, des méthodes de fiabilité dynamique (en anglais, « *dynamic reliability* » ou « *probabilistic dynamic* ») ont alors été développées afin de prendre explicitement en compte les influences du temps, les évolutions du processus, et les actions humaines, sur les états fonctionnels des systèmes, et les scénarios accidentels. La première de ces approches à avoir été proposée est la *dynamical logical analytical methodology* (DYLAM) [AAm84, PCa86]. Celle-ci utilise une discrétisation du temps pour simuler toutes les séquences d'évènements, couplées avec les évolutions du processus. Ensuite, plusieurs autres méthodes ont émergé permettant des modélisations de la fiabilité dynamique :

- les *discrete dynamic event trees* (DDET), qui incluent DYLAM [AAm84, PCa86, GCo96], DETAM [CAc93], ADS [KHs96], MCDET [MKl06], et ADAPT [AHa08] ;
- les *event sequence diagrams* (ESD) [LPi83], en particulier ceux étendus à la fiabilité dynamique [SSw99, SSw00] ;
- la *GO-FLOW methodology* [TMa88, TMa96] ;
- les arbres de défaillance et les diagrammes de fiabilité avec des caractéristiques dynamiques [MCe02, MBo03, SDi06], et les réseaux bayésiens dynamiques équivalents [SSh08] ;
- la *dynamic flowgraph methodology* (DFM) [CGa95, MYa98] ;
- les réseaux de Petri avec des caractéristiques stochastiques [YDu97b, CKe04], et colorées [PSk08] ;
- des modèles markoviens, combinés à la *cell-to-cell mapping technique* (CCMT) pour discrétiser le temps et les autres variables continues [TAl87, TAl91], ou avec l'extension en temps continu, nommée *continuous cell-to-cell mapping technique* (CCCMT) [BTo96] ;
- des modèles directement basés sur les *piecewise-deterministic Markov Processes* (PDMP), pour effectuer des simulations de Monte Carlo [HZh08], et des approches par algorithmes déterministes [WLa10a, WLa10b] ;
- des approches directes de simulations de Monte Carlo [CSm92, MMa96, PLa97], des simulations par évènements discrets [NSi94], et des simulations effectuées par *automate stochastique hybride* (ASH) [NBr09, GPe10].

La plupart de ces méthodes ont été présentées, comparées, et discutées par T. Aldemir *et al.* [TAl94], N. Siu [NSi94], et P.E. Labeau *et al.* [PLa00], et appliquées au problème maintenant bien connu « du réservoir » [TAl87] : DDET [NSi94], *GO-FLOW methodology* [NSi94], réseaux de Petri [YDu97b, PSk08], modèles markoviens [TAl87, TAl91], PDMP [HZh08, WLa10a], et méthodes de Monte Carlo [MMa96, NBr09] ; ou à des systèmes issus de réacteurs nucléaires : DDET [AAm84, PCa86, GCo96, CAc93, KHs96, MKl06], ESD [SSw00], arbres de défaillance dynamiques [MCe02], DFM [JKi09, TAl10], modèles markoviens [JKi09, TAl10], et méthodes de Monte Carlo [CSm92, PLa97].

La formalisation mathématique de la fiabilité dynamique a été établie sous le nom de la théorie des *continuous event trees* (CET) [JDe92b]. Cette dernière a introduit deux types de variables utilisés pour définir l'état complet du système :

- les variables (discrètes) d'état des composants (par exemple, état *opérant*, état de *défaillance*) ;
- les variables (continues) physiques du processus (par exemple, niveaux, pression, température) ;

Les changements d'état des composants sont supposés stochastiques, définis par des taux de transition, et dépendent des variables du processus. Réciproquement, les évolutions des variables du processus sont déterminées par des équations différentielles (non-stochastiques) du premier ordre, en fonction de l'état des composants. L'état des composants et les variables du processus sont ainsi mutuellement dépendants, et suivent un processus (markovien) déterministe par morceaux (PDP) [MDa84, MDa93]. Sous des hypothèses markoviennes, des équations de Chapman-Kolmogorov ont été utilisées pour exprimer la densité de probabilité de l'état complet du système en fonction du temps [JDe92b, JDe96]. Plusieurs travaux ont alors cherché à manipuler la distribution de probabilité qui en résulte, en utilisant la méthode des moments [JDe95], ou en caractérisant la distribution marginale [PLa96, CCo40b] ; et des solutions numériques ont été apportées [CCo06a]. Le formalisme mathématique a également été étendu pour y introduire des opérations humaines, par l'utilisation de variables additionnelles [JDe92a].

Plus récemment, l'utilisation de systèmes à fonctionnalités numériques pour des applications liées à la sécurité a aussi introduit de nouvelles problématiques pour la modélisation de la fiabilité dynamique, notamment de par certaines interactions spécifiques entre les éléments du système [TAl06, TAl10, AAl10]. Depuis la fin des années quatre-vingt-dix, ces considérations ont pris de l'ampleur, en particulier pour les centrales nucléaires où l'instrumentation analogique devient obsolète et est remplacée peu à peu par des systèmes numériques [TAl06, EZi09, AAl10]. Des problématiques similaires sont également apparues, encore plus tôt, dans l'industrie aérospatiale qui utilise de nombreux systèmes de contrôle à base de logiciels [DZh07]. Des exemples de ce type de système sont les CTI qui peuvent notamment « coopérer » en s'échangeant des informations (cf. Section I.3, ainsi que les exemples présentés dans les Section IV.2.1 et IV.3.3).

Avant tout, il convient de noter que, malgré le consensus sur les besoins en termes de méthodes de fiabilité dynamique [TAl96], et en particulier pour les systèmes complexes et à fonctionnalités numériques, ces approches n'ont pas encore pleinement pénétré les champs d'applications industrielles [PLa00]. Les raisons avancées à cela sont les aspects théoriques qui sont assez complexes, et le manque d'une plateforme générique pour effectuer de telles analyses. En particulier, les outils logiciels correspondants sont presque tous entièrement dépendants des applications considérées [PLa00]. De plus, parce qu'une théorie générale doit être respectée afin de comparer différentes approches [JDe96], il conviendrait que tout nouveau développement dans le domaine de la fiabilité dynamique :

- soit compatible avec le formalisme mathématique des *continuous event trees* défini par J. Devooght et C. Smidts [JDe92b] ;
- fournisse une approche générique, appropriée par nature aux plus larges champs d'applications, et avec un minimum d'adaptations nécessaires.

La Section IV.2 présente un exemple introductif de système de contrôle-commande intégrant des CTI « coopérants ». Dans cette première approche, seules les interactions entre les CTI sont prises en compte. Ensuite, la Section IV.3 développe une approche complète de fiabilité dynamique en y incluant à la fois les interactions entre les éléments du système (et en particulier les CTI) et le processus contrôlé. Pour cela, le formalisme mathématique de la fiabilité dynamique est étendu afin de prendre en compte les particularités des CTI, et une modélisation formalisée, à caractère « générique », est proposée. Un cas d'étude relativement complet permet alors d'illustrer cette approche. Les approches utilisées dans les Sections IV.2 et IV.3 ont pour point commun d'exploiter des réseaux de Petri. Ces derniers sont brièvement présentés dans la section suivante.

IV.1.3. Quelques Rappels sur les Réseaux de Petri

Les réseaux de Petri sont des outils de modélisation et d'évaluation à la fois graphiques et mathématiques. À partir des graphes constituant les réseaux de Petri, il est par exemple possible d'obtenir des équations d'états et des modèles mathématiques qui gouvernent le système [TMu89]. Un réseau de Petri « ordinaire » est constitué de places (cercles) et de transitions (rectangles), tels que décrit sur la Figure IV.1.1. Des connections (arcs orientés) peuvent relier une place à une transition (arc d'entrée) ou vice-versa (arc de sortie), et peuvent être « valuées » (autrement, le poids est considéré comme étant égal à *1*). Ces réseaux de places-transitions sont ainsi des graphes bipartis et orientés. Les places peuvent contenir des jetons (petits cercles pleins) qui sont « déplacés » par l'intermédiaire des transitions, lorsque ces dernières sont franchies. Une transition est franchissable si chacune de ses places d'entrée (liées à la transition par un arc d'entrée) contient un nombre de jetons égal ou supérieur aux valeurs des arcs d'entrée correspondants. Franchir une transition consiste alors en deux étapes : retirer dans chacune des places d'entrée un nombre de jetons égal aux valeurs des arcs d'entrée associés ; puis déposer dans chacune des places de sortie un nombre de jetons égal aux valeurs des arcs de sortie associés (cf. Figure IV.1.1). Plus de détails sur ces règles et ces définitions, des exemples, ainsi que des propriétés, peuvent être trouvés dans de nombreuses références [JPe81, TMu89].

Généralement, les places d'un réseau de Petri représentent des objets et des conditions, les jetons spécifient les valeurs de ces objets et conditions, et les transitions modélisent les activités du système. Afin de modéliser des systèmes complexes, plusieurs extensions des réseaux de Petri ont été développées, qui incluent notamment des propriétés colorées, temporisées, et stochastiques. Dans les réseaux de Petri colorés [KJe02], différents types (couleurs) de jetons sont représentés au sein du même graphe, facilitant ainsi la modélisation et améliorant sa clarté. Plus généralement, des valeurs peuvent être attribuées à chaque jeton, et modifiées lors des franchissements de transitions ou lorsque les jetons restent dans les places (jetons « vieillissants » [VVo04]). Les politiques de franchissement des transitions peuvent également être fonction des valeurs des jetons. La dimension temporelle est introduite dans les réseaux de Petri temporisés, par l'utilisation de temps de séjour des jetons dans les places, et/ou de délais pour franchir les transitions. Dans les réseaux de Petri stochastiques [FBa02b], ces délais sont des variables aléatoires. Parmi les extensions relativement flexibles des réseaux de Petri stochastiques se trouvent les *stochastic activity networks* (SAN) [JMe85]. Lorsqu'un réseau de Petri inclut à la fois des transitions immédiates et temporisées, ils sont également qualifiées de réseaux de Petri (stochastiques) généralisés.

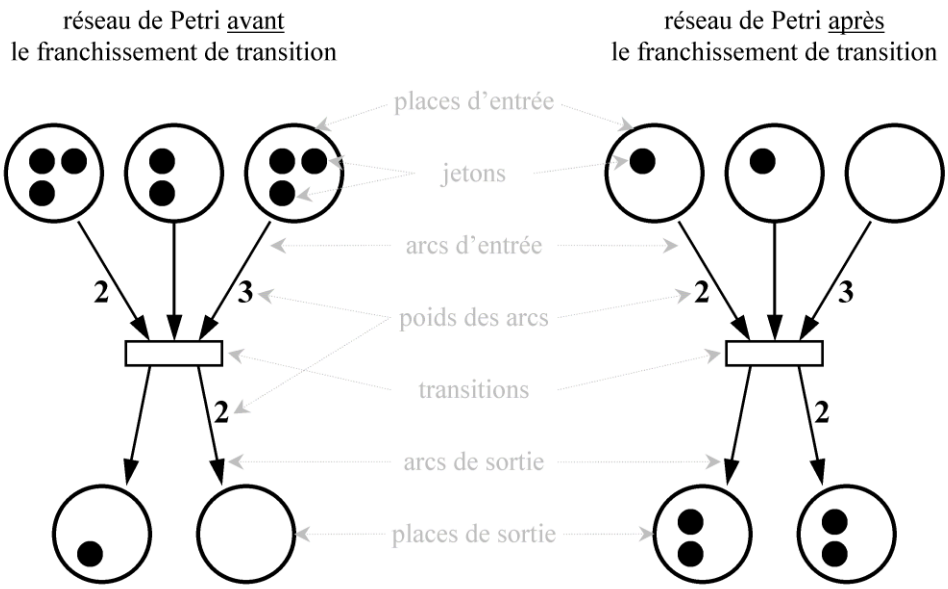

Figure IV.1.1. Exemple de réseau de Petri, et illustration d'un franchissement de transition

Une des principales difficultés des réseaux de Petri est alors de répondre efficacement à la complexité du problème, c'est-à-dire que plus le modèle est général, et moins il est maniable lors des analyses [TMu89]. Par exemple, sous certaines conditions, les réseaux de Petri stochastiques peuvent être analysés par l'intermédiaire de chaînes de Markov [FBa02b]. Pour des problèmes plus complexes et plus généraux, les réseaux de Petri peuvent être directement utilisés pour effectuer des analyses qualitatives, mais les analyses quantitatives nécessitent souvent des simulations de Monte Carlo, ce qui peut alors exiger un temps parfois très long, et impliquer quelques problèmes de justification des résultats obtenus. Des informations très complètes sur les réseaux de Petri peuvent, par exemple, être trouvées sur le site Internet *Petri Nets World* [Pet10].

IV.2. SYSTÈMES DE CONTRÔLE-COMMANDE INTÉGRANT DES « CAPTEURS-TRANSMETTEURS INTELLIGENTS » COOPÉRANTS

IV.2.1. Exemple de SCC à trois CTI Coopérants

IV.2.1.1. Système de base à trois capteurs-transmetteurs redondants

Tout d'abord, un système de contrôle-commande (SCC) « de base » est considéré. Celui-ci est constitué de trois capteurs-transmetteurs redondants, c'est-à-dire qu'ils mesurent les mêmes grandeurs (dont les valeurs sont les mêmes). L'architecture matérielle de ce système est décrite sur la Figure IV.2.1 (les aspects concernant le réseau de communication ne relèvent pas du « système de base » mais sont introduits dans la section suivante).

Chacun des trois capteurs-transmetteur (nommés dans la suite CTI 1, CTI 2, et CTI 3) effectue à la fois une mesure du mesurande (quantité dont on souhaite évaluer la valeur), et de facteurs d'influences (quantités qui ont un effet sur l'évaluation du mesurande), en utilisant respectivement un transducteur principal et auxiliaire. Les résultats de mesures, en tant que fonctions du mesurande et des facteurs d'influence, sont ensuite calculés par une unité de traitement. De plus, des autodiagnostics sont disponibles pour chacun de ces sous-systèmes (transducteur principal, transducteur auxiliaire, unité de traitement), selon une couverture de diagnostic qui est la probabilité de détecter une défaillance du sous-système lorsque celle-ci se produit. Enfin, les résultats de mesure sont transmis à une unité centrale de contrôle, en utilisant une interface de communication. La transmission du signal peut se faire soit analogiquement (par exemple, en utilisant le principal standard industriel, c'est-à-dire un signal analogique en 4-20 mA), soit numériquement (par exemple, en utilisant des réseaux de terrain ou une communication sans-fil).

Si au moins une défaillance d'un des sous-systèmes du CTI est détectée par autodiagnostic, un signal d'erreur (par exemple, supérieur à 20 mA, ou inférieur à 4 mA, pour un signal analogique) est transmis à la place d'un signal qui représente les résultats de mesure. Si au moins une défaillance d'un des sous-systèmes du CTI s'est produite, mais qu'aucune défaillance n'a été détectée par autodiagnostic, un signal qui correspond à des conditions normales d'opération (c'est-à-dire qui ne correspond pas à la détection d'un évènement dangereux) est transmis, ce qui signifie que seules des *défaillances dangereuses* sont considérées, et aucun *déclenchement intempestif*. L'unité centrale de contrôle est alors capable d'activer une fonction de sécurité qui est réalisée par des actionneurs (qui ne relèvent pas du présent cas d'étude), si au minimum la majorité des signaux reçus, et qui ne sont pas des signaux d'erreur, représente des résultats de mesure corrects. La logique de traitement de l'unité centrale de contrôle est ainsi *2*-sur-*3* si tous les CTI sont diagnostiqués comme « *opérants* » (c'est-à-dire qu'ils ne transmettent pas des signaux d'erreurs), *1*-sur-*2* si exactement deux CTI sont diagnostiqués comme « *opérants* », et *1*-sur-*1* si un seul CTI est diagnostiqué comme « *opérant* ». Enfin, si aucun CTI n'est diagnostiqué comme « *opérant* », alors l'unité centrale de contrôle fournit une information d'erreur.

Chaque CTI a ainsi trois états fonctionnels possibles : *opérant* si tous ses sous-systèmes sont opérants ; *défaillance détectée* si au moins une défaillance de l'un de ses sous-systèmes s'est produite et qu'elle a été détectée par autodiagnostic ; et *défaillance non détectée* si au moins une

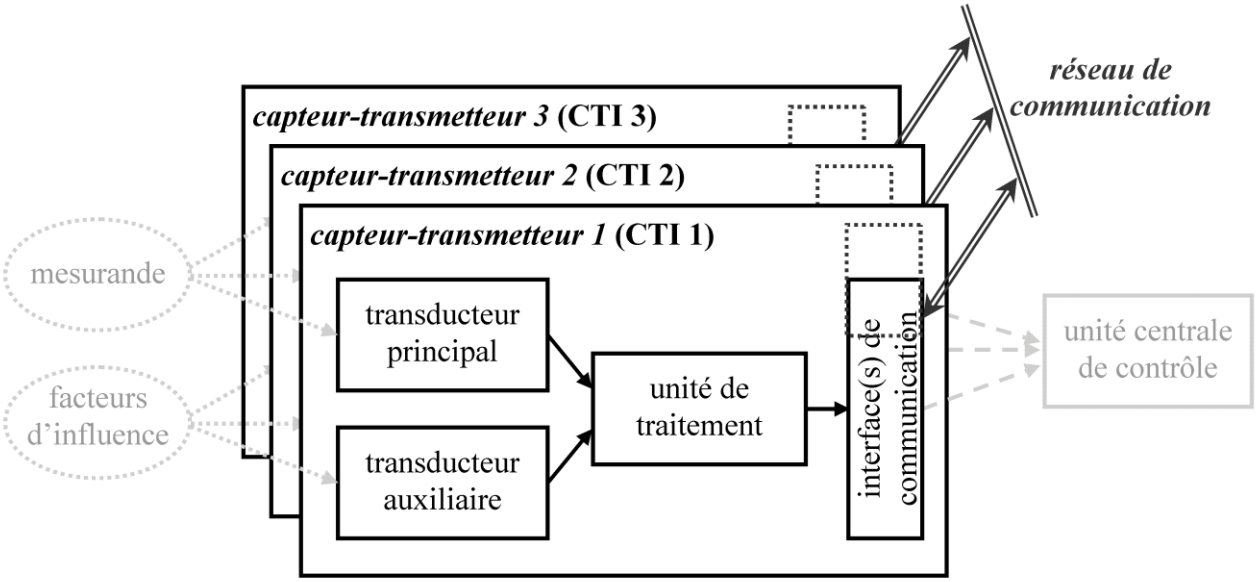

Figure IV.2.1. Architecture matérielle du système de contrôle-commande (SCC)

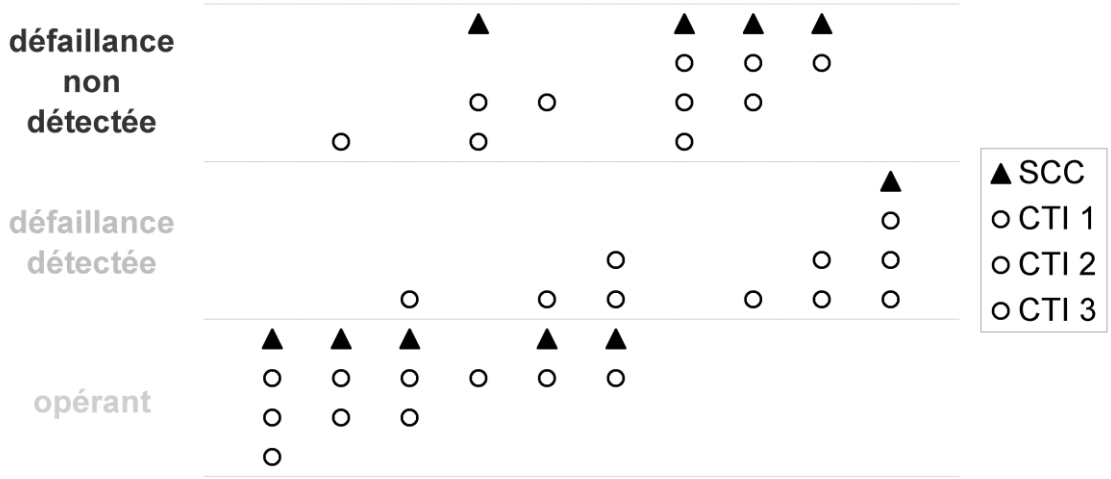

Figure IV.2.2. États fonctionnels du système de contrôle-commande (SCC),
en fonction des états fonctionnels des trois « capteurs-transmetteurs intelligents » (CTI),
(chaque configuration possible est donnée par colonne)

défaillance de l'un de ses sous-systèmes s'est produite et qu'aucune d'elles n'a été détectée par autodiagnostic. L'état fonctionnel du SCC est alors fonction des états fonctionnels des trois CTI, tel que décrit sur la Figure IV.2.2 (où chaque configuration possible d'états fonctionnels des CTI et du SCC est donnée par colonne). De par la logique de traitement introduite précédemment, le SCC est dans un état *opérant* si au moins deux CTI sont dans des états *opérants*, ou si un seul CTI est dans un état *opérant* mais qu'au minimum un autre CTI est dans un état de *défaillance détectée* ; le SCC est dans un état de *défaillance détectée* si les trois CTI sont dans un état de *défaillance détectée* ; et le SCC est dans un état de *défaillance non détectée* dans tous les autres cas.

IV.2.1.2. Du système de base au système en réseau

Un réseau de communication est ici considéré entre les trois CTI du SCC. Cette communication peut, par exemple, être assurée par l'ajout d'une interface de communication sans-fil, indépendamment de la communication entre les CTI et l'unité centrale de contrôle. Si la communication entre les CTI n'est pas indépendante de la communication avec l'unité centrale, les problématiques présentées dans la Section IV.1.1 doivent être prises en compte. Ce cas n'est cependant pas considéré dans la suite, la sûreté de fonctionnement des réseaux de communication n'étant pas prise en compte ici.

Ce module supplémentaire de communication permet aux CTI de s'échanger entre eux plusieurs types d'informations : l'identifiant du CTI, la valeur évaluée du mesurande (telle qu'obtenue en sortie du transducteur principal), la valeur d'autodiagnostic du transducteur principal, la valeur évaluée des facteurs d'influence (telle qu'obtenue en sortie du transducteur auxiliaire), la valeur d'autodiagnostic du transducteur auxiliaire, les résultats de mesure (tels qu'obtenus en sortie de l'unité de traitement), la valeur d'autodiagnostic de l'unité de traitement, ainsi qu'un résultat de diagnostic compilé, calculé par l'unité de traitement à partir des trois valeurs d'autodiagnostics. Ce résultat de diagnostic compilé détermine la nature du signal transmis à l'unité centrale de contrôle. Si ce dernier est « confiant », alors le signal transmis à l'unité centrale de contrôle représente les résultats de mesure, s'il est « non confiant », alors le signal transmis est un signal d'erreur.

Un CTI peut être sollicité selon deux types de demande. Lorsqu'un CTI est sollicité seul, suivant un procédé cyclique (chaque CTI est sollicité à tour de rôle), le type de demande correspondant est *cyclique*. Lorsque plus d'un CTI est sollicité au même instant, le type de demande correspondant est *parallèle*. Parce qu'un seul CTI à la fois peut utiliser le réseau de communication afin d'éviter les problèmes d'instabilité du système (cf. Section IV.1.1), un CTI n'est autorisé à transmettre des informations aux autres CTI que lorsqu'il est sollicité selon un type de demande *cyclique*.

À tour de rôle (selon un intervalle de temps notée c), chaque CTI effectue donc ses évaluations (valeurs évaluées du mesurande et des facteurs d'influence, résultats de mesures, valeurs d'autodiagnostics, résultat de diagnostic compilé) selon un type de demande *cyclique*, puis transmet ses informations aux autres CTI du réseau. Ces derniers effectuent alors, à leur tour (après un certain délai noté d, et avec $d < c$), leurs évaluations selon un type de demande *parallèle*. De plus, à chaque fois qu'un CTI est sollicité (soit selon un type de demande *cyclique* ou *parallèle*), il transmet un signal à l'unité centrale de contrôle (soit un signal qui représente les résultats de mesure, soit un signal d'erreur, selon le résultat de diagnostic compilé). Ce procédé de sollicitations des CTI peut être appliqué à un SCC constitué de n'importe quel nombre de CTI. Pour le présent cas d'étude, le SCC est constitué de trois CTI et le cycle des sollicitions correspondant est décrit dans le Tableau IV.2.1.

Tableau IV.2.1. Cycle des sollicitations pour les trois « capteurs-transmetteurs intelligents » (CTI) du système de contrôle-commande (SCC)

temps[a]	sollicitation	signal ou informations transmis
$t_0 = 0$	.	.
$t_1 = t_0$	demande *cyclique* du CTI 1	signal à l'unité centrale de contrôle informations aux CTI 2 et CTI 3
$t_2 = t_0 + d$	demande *parallèle* du CTI 2 demande *parallèle* du CTI 3	signal à l'unité centrale de contrôle signal à l'unité centrale de contrôle
$t_3 = t_1 + c$	demande *cyclique* du CTI 2	signal à l'unité centrale de contrôle informations aux CTI 1 et CTI 3
$t_4 = t_2 + c$	demande *parallèle* du CTI 1 demande *parallèle* du CTI 3	signal à l'unité centrale de contrôle signal à l'unité centrale de contrôle
$t_5 = t_3 + c$	demande *cyclique* du CTI 3	signal à l'unité centrale de contrôle informations aux CTI 1 et CTI 2
$t_6 = t_4 + c$	demande *parallèle* du CTI 1 demande *parallèle* du CTI 2	signal à l'unité centrale de contrôle signal à l'unité centrale de contrôle
$t_7 = t_5 + c$	demande *cyclique* du CTI 1	signal à l'unité centrale de contrôle informations aux CTI 2 et CTI 3
$t_8 = t_6 + c$	demande *parallèle* du CTI 2 demande *parallèle* du CTI 3	signal à l'unité centrale de contrôle signal à l'unité centrale de contrôle
etc.		

[a]Avec la constante *c* qui est la période entre deux sollicitations de CTI selon une demande *cyclique*, et la constante *d* qui est un délai tel que $d < c$.

IV.2.1.3. Algorithmes pour CTI coopérants

Basées sur deux algorithmes, des procédures sont proposées afin d'améliorer des critères de sûreté de fonctionnement du SCC en tirant avantage de coopérations entre les CTI. Ces deux algorithmes sont nommés *algorithme de secours* et *algorithme de contraste*. Le premier concerne les mesures du mesurande et des facteurs d'influence, effectuées par les transducteurs principaux et auxiliaires. Le second concerne les résultats de diagnostic compilé, effectués par les unités de traitement. Ces algorithmes sont ainsi fonctionnellement indépendants et peuvent être utilisés isolément ou conjointement. Lorsqu'un CTI est sollicité, il peut alors suivre un seul ou les deux algorithmes proposés. Ces derniers utilisent les informations transmises par les autres CTI, et sont basés sur les valeurs d'autodiagnostics des sous-systèmes des CTI afin de comparer, évaluer, et remplacer des valeurs requises lors des traitements. Enfin, ces algorithmes peuvent être exploités quel que soit le nombre de CTI présents dans le réseau.

Le premier algorithme, nommé *algorithme de secours*, est utilisé pour remplacer une valeur qui a été obtenue pour un mesurande (respectivement, pour des facteurs d'influence), par la valeur correspondante parmi des informations reçues (provenant d'un autre CTI, et qui a été sollicité selon un type de demande *cyclique*), si cette dernière valeur est jugée plus « confiante » d'après les valeurs d'autodiagnostics des transducteurs principaux (respectivement, des transducteurs auxiliaires). De plus, un procédé de mémorisation est utilisé afin de retenir la valeur jugée la plus « confiante » (pour les mesurandes et les facteurs d'influence) d'après les valeurs d'autodiagnostics, parmi les dernières informations reçues provenant des autres CTI. La procédure basée sur l'*algorithme de secours* est donc la suivante :

Lorsqu'un CTI est sollicité et suit l'*algorithme de secours*,

1. effectuer ses évaluations (valeurs évaluées du mesurande et des facteurs d'influence, valeurs d'autodiagnostics du transducteur principal et auxiliaire), indépendamment des informations reçues provenant d'autres CTI ;
2. lire les informations reçues provenant du dernier CTI transmettant des informations aux autres CTI ;
3. lire les dernières informations mémorisées ;
4. remplacer les dernières informations mémorisées par les informations reçues, si les deux identifiants des CTI sont les mêmes, ou si les valeurs évaluées du mesurande et/ou des facteurs d'influence sont jugées plus « confiantes » d'après les valeurs d'autodiagnostics ;
5. l'unité de traitement du CTI calcule les résultats de mesure en utilisant les valeurs évaluées du mesurande et des facteurs d'influence qui sont jugées les plus « confiantes » d'après les autodiagnostics, parmi les évaluations du CTI et les dernières informations mémorisées, si le type de demande du CTI sollicité est *parallèle*.

Le second algorithme, nommé *algorithme de contraste*, est utilisé pour remplacer un résultat de diagnostic compilé qui est calculé par l'unité de traitement, par un résultat de diagnostic obtenu par des comparaisons de résultats de mesure. Lorsqu'un CTI est sollicité, il effectue ses évaluations et compare ensuite ses résultats de mesure avec les résultats de mesure issus des informations reçues (provenant d'un autre CTI, et qui a été sollicité selon un type de demande *cyclique*). Si deux comparaisons consécutives de résultats de mesure, effectuées avec des informations reçues jugées « confiantes » d'après le résultat de diagnostic compilé, ont conclu que les résultats de mesure étaient les mêmes (respectivement, pas les mêmes), alors le résultat de diagnostic compilé est remplacé par « confiant » (respectivement, « non confiant »). La procédure basée sur l'*algorithme de contraste* est donc la suivante :

Lorsqu'un CTI est sollicité et suit l'*algorithme de contraste*,

1. effectuer ses évaluations (résultats de mesures, résultat de diagnostic compilé), indépendamment des informations reçues provenant d'autres CTI ;
2. lire les informations reçues provenant du dernier CTI transmettant des informations aux autres CTI ;
3. comparer les résultats de mesure issus des évaluations du CTI avec les résultats de mesure issus des informations reçues, et mémoriser l'identifiant du CTI issu des informations reçues avec une étiquette qui représente la correspondance des résultats de mesure (« positive » s'ils sont les mêmes, « négative » sinon), si le résultat compilé de diagnostics issu des informations reçues est « confiant » ;
4. remplacer le résultat de diagnostic compilé issu des évaluations de CTI par « confiant » (respectivement, « non confiant »), si les deux derniers différents identifiants de CTI mémorisés ont tous deux une étiquette « positive » (respectivement, « négative »), et si le type de demande du CTI sollicité est *parallèle*.

IV.2.2. Modélisation en Réseaux de Petri appliquée au SCC

IV.2.2.1. Le choix des réseaux de Petri et de l'outil logiciel

Afin de modéliser le système en y incluant la coopération entre les CTI du réseau, et ensuite d'être en mesure d'évaluer des critères de sûreté de fonctionnement, les réseaux de Petri colorés et stochastiques ont été perçu comme un outil relativement intuitif et performant (cf. Section IV.1.3). Par exemple, des approches basées sur des réseaux de Petri ont déjà été utilisées dans plusieurs études connexes [PPo04, RGh06, RGh11, PBa03, JPi02, JCa99] (cf. Section IV.1.1). Tandis que les propriétés stochastiques sont requises pour modéliser des défaillances aléatoires et des autodiagnostics imparfaits, les caractéristiques colorées permettent de représenter de façon compacte et assez intuitive plusieurs types d'informations (par exemple, des valeurs de mesure ou d'autodiagnostics, des résultats), et des propriétés (par exemple, des états fonctionnels, des justesses de valeurs ou de résultats).

Le logiciel CPN Tools [CPN10] a alors été choisi pour modéliser le SCC. Il s'agit d'un logiciel gratuit développé par l'université d'Aarhus pour éditer, simuler, et analyser des réseaux de Petri colorés [CPN10]. Parmi certaines de ses caractéristiques qui ont guidé ce choix, CPN Tools est conçu pour manipuler des réseaux de Petri colorés, temporisés ou non, et, bien que les aspects stochastiques ne soient pas directement pris en compte, les possibilités de déclaration de variables et de fonctions permettent d'inclure ces propriétés [KJe07]. De plus, des réseaux de Petri « hiérarchiques » peuvent être créés en attribuant à une transition un réseau de Petri séparé, ou en fusionnant des places, ce qui est particulièrement utile pour modéliser des systèmes composés de plusieurs éléments similaires. Pour le côté pratique, certaines facilités d'utilisation sont offertes par l'interface utilisateur, l'éditeur graphique, la vérification automatique de la syntaxe, et les messages d'erreurs contextuels [ARa03]. Enfin, pour effectuer des analyses quantitatives, des simulations de Monte Carlo sont requises.

IV.2.2.2. Modélisation du SCC via le logiciel CPN Tools

Le réseau de Petri coloré et stochastique utilisé pour modéliser les transducteurs principaux des CTI est décrit sur la Figure IV.2.3. Ce dernier est ici proposé en tant qu'exemple, afin d'illustrer la

modélisation via le logiciel CPN Tools. Le réseau de Petri des transducteurs auxiliaires est similaire à celui de la Figure IV.2.3, excepté pour certains paramètres et noms de variables ou de places, et n'est donc pas décrit sur une figure supplémentaire. D'autres réseaux de Petri (non décrits ici) ont également été utilisés pour modéliser les unités de traitement, les CTI dans leur ensemble (qui incluent hiérarchiquement les réseaux de Petri des transducteurs principaux et auxiliaires, des unités de traitement, et des interfaces de communication), et le SCC (qui inclut hiérarchiquement trois réseaux de Petri de CTI).

La hiérarchie entre les réseaux de Petri est définie par des étiquettes rectangulaires attachées en bas à gauche des places (cf. Figure IV.2.3). Par exemple, l'étiquette « out » de la place « SubInformation » représente un lien de sortie, et l'étiquette « in » de la place « Demand » représente un lien d'entrée, vers des réseaux de Petri « extérieurs », c'est-à-dire que ces places ainsi étiquetées sont associées à des places d'autres réseaux de Petri. L'étiquette « I/O » représente à la fois un lien d'entrée et de sortie, et d'autres étiquettes telles que « ExDigitInfo » sont attribuées à des places qui sont communes à plusieurs réseaux de Petri (ces places sont dites « fusionnées »).

Sur la Figure IV.2.3, la chaîne de mesure est représentée par les places « Measurand », « Measurement », et « SubInformation » (les jetons y prennent respectivement la valeur du mesurande, la valeur évaluée du mesurande, et la valeur évaluée du mesurande associé à la valeur de l'autodiagnostic du transducteur) ; les états du transducteur et de l'autodiagnostic sont représentés par les places « State » et « Diag » (les jetons y prennent respectivement la valeur *100* pour « StateIsOk » ou « SelfDiagIsOk », et la valeur *0* pour « StateIsFailed » ou « SelfDiagIsFailed ») ; les aspects aléatoires des défaillances sont représentés par les places « InitFail » et « Failure » (une défaillance se produit lorsque la transition « ToFail » est franchie, changeant alors l'état du transducteur, et celui de l'autodiagnostic selon la couverture de diagnostic) ; la gestion du cycle des sollicitations est obtenue par les places « Demand », « DemandMemInfo », « DemandDigitInfo », et « Available » (les jetons y sont utilisés pour solliciter une demande et y préciser le type de celle-ci) ; et les informations échangées entre les CTI, ainsi que la gestion des procédures basées sur l'*algorithme de secours* (seul algorithme concerné par la Figure IV.2.3), sont représentés par toutes les autres places, décrites dans la partie inférieure de la Figure IV.2.3.

Le nombre de jetons présents dans une place non vide est donné par le cercle plein qui lui est attaché, et les valeurs des jetons sont précisées dans le rectangle à coté. La notation « 1` » signifie qu'il y a un jeton, « 2` » signifie qu'il y a deux jetons, etc. Une place ne peut contenir qu'une seule sorte de jeton qui est définie par le type de couleur donné en lettres majuscules en bas de la place. Le nombre initial de jetons dans une place est défini par les valeurs initiales des jetons données en lettres minuscules en haut de la place. Par exemple, la place « State » de la Figure IV.2.3 contient un seul jeton, dont la couleur est de type « STATE » (qui correspond à des nombres entiers), et qui a la valeur *100*, qui correspond à la valeur initiale « *StateIsOk* » (*StateIsOk = 100*). D'autres types de couleur peuvent être « incolores », par exemple la place « InitFail » contient des jetons dont la couleur est de type « FAILURE », et qui prennent des valeurs qui ne sont représentées que par le symbole « () » ; ou alors être définies par un ensemble, par exemple la place « DemandType » contient des jetons dont la couleur est de type « TYPEofDEMAND », et qui prennent soit la valeur « *c* » (pour une demande de type *cyclique*) ou la valeur « *p* » (pour une demande de type *parallèle*) ; ou encore être associées à plusieurs variables, par exemple la place « Exchanged DigitInfo » contient des jetons dont la couleur est de type « DIGITINFO » et qui regroupe sept entiers naturels. Lorsqu'une couleur est temporisée, les valeurs de jetons correspondants sont données avec le symbole « @ » suivi d'un nombre entier qui représente le prochain temps où le jeton deviendra

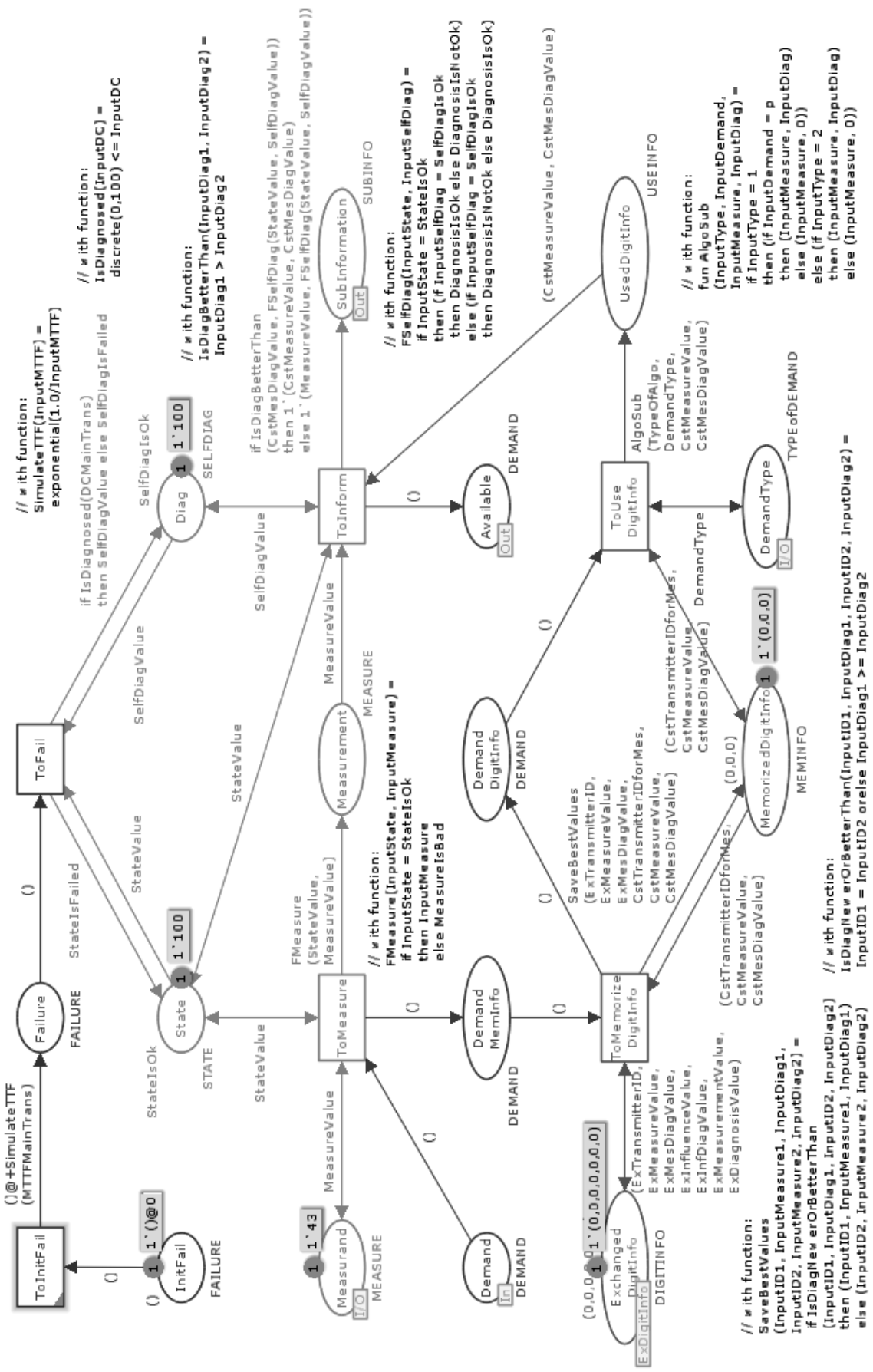

Figure IV.2.3. Réseau de Petri coloré et stochastique pour les transducteurs principaux des CTI

disponible (avant cet instant, le jeton ne peut pas être manipulé par une transition, c'est-à-dire qu'il ne peut pas être utilisé pour franchir une transition).

Un arc d'entrée (d'une place vers une transition) précise le nombre de jetons (« 1` » par défaut) à retirer dans la place d'entrée, avec le nom de la variable qui prend la valeur du jeton retiré. Un arc de sortie (d'une transition vers une place) précise le nombre de jetons à déposer dans la place de sortie, avec une variable qui donne sa valeur au jeton déposé. Cette dernière variable peut être une fonction des variables d'entrée (ces fonctions sont précisées sur la Figure IV.2.3 par les textes commençant par « // with function: »). Par exemple, le jeton qui est déposé dans la place « Measurement » de la Figure IV.2.3 prend la valeur de la variable « *MeasureValue* » si la variable « *StateValue* » est égale à « *StateIsOk* », et la valeur « *MeasureIsBad* » sinon. En utilisant des arcs bidirectionnels (par exemple, entre la place « Measurand » et la transition « ToMeasure »), le jeton de la place d'entrée reste inchangé une fois la transition franchie, mais la valeur de ce jeton peut être utilisée comme donnée d'entrée pour des fonctions définissant des variables de sortie. Pour les jetons temporisés, les délais (nombres après le symbole « @ ») peuvent également être modifiés par les arcs de sortie. Par exemple, lorsque la transition « ToInitFail » est franchie, le jeton déposé dans la place « Failure » a un délai qui est augmenté par une variable aléatoire qui suit une distribution exponentielle de moyenne égale à « *MTTFMainTrans* ». Les paramètres d'entrée utilisés pour les fonctions aléatoires sont donnés dans le Tableau IV.2.2. À noter qu'une redondance passive a été considérée pour les unités de traitement des CTI, c'est-à-dire que lorsque la première défaillance d'une unité de traitement se produit, il y a une certaine probabilité d'activation de la redondance passive qui, le cas échéant, prolonge la durée de vie de l'unité de traitement (cf. paramètres donnés dans le Tableau IV.2.2).

IV.2.3. Évaluation des critères de Disponibilité et de Sécurité appliquée au SCC

IV.2.3.1. Évaluation par simulations de Monte Carlo

Les temps de bon fonctionnement des sous-systèmes des CTI (transducteurs auxiliaires et principaux, unités de traitement) suivent des distributions exponentielles dont les moyennes sont données dans le Tableau IV.2.2 (d'autres distributions peuvent également être considérées). Lorsque la défaillance d'un sous-système se produit, elle est détectée par autodiagnostic selon une probabilité qui est constante et égale à la couverture de diagnostic donnée dans le Tableau IV.2.2. Les couvertures de diagnostic sont les mêmes pour l'ensemble des sous-systèmes des transmetteurs, et cinq valeurs sont considérées afin d'étudier l'impact de ce paramètre sur la sûreté de fonctionnement du SCC, et selon les algorithmes proposés. Parce qu'aucune action de maintenance n'est considérée sur toute la période d'étude, les critères utilisés pour évaluer la disponibilité et la sécurité du système sont des pourcentages de temps que le SCC passe dans certains états fonctionnels au cours des *10 000* premières unités de temps. La disponibilité est alors calculée comme la probabilité (pourcentage de temps) que le SCC soit dans un état *opérant*, et la sécurité est calculée comme la probabilité (pourcentage de temps) que le SCC ne soit pas dans un état de *défaillance non détectée*.

Quatre cas sont considérés, selon que l'*algorithme de secours* et/ou l'*algorithme de contraste* sont utilisés ou non. Pour chacun de ces cas, différentes couvertures de diagnostic pour l'ensemble des sous-systèmes des CTI sont également considérées : toutes égales à *0.00* dans le cas *CD00* (aucune

Tableau IV.2.2. Paramètres de fiabilité du système de contrôle-commande (SCC)

paramètre	valeur
temps moyen avant défaillance des transducteurs principaux	*5 000* unités de temps[a]
temps moyen avant défaillance des transducteurs auxiliaires	*5 000* unités de temps[a]
temps moyen avant défaillance des unités de traitement	*5 000* unités de temps[a]
temps moyen avant défaillance des redondances passives des unités de traitement	*2 500* unités de temps[a]
couverture de diagnostic des transducteurs principaux	*0.00*, *0.25*, *0.50*, *0.75*, ou[b] *1.00*
couverture de diagnostic des transducteurs auxiliaires	*0.00*, *0.25*, *0.50*, *0.75*, ou[b] *1.00*
couverture de diagnostic des unités de traitement	*0.00*, *0.25*, *0.50*, *0.75*, ou[b] *1.00*
probabilité d'activation des redondances passives des unités de traitement, lorsque leurs premières défaillances se produisent	*0.75*

[a]Ces temps moyens sont utilisés pour simuler des défaillances selon des distributions exponentielles.
[b]Ces couvertures de diagnostic correspondent aux probabilités de détecter les défaillances des sous-systèmes concernés lorsqu'elles se produisent. Toutes les couvertures de diagnostic sont égales, et ces cinq valeurs sont considérées.

défaillance n'est détectée), toutes égales à *0.25* dans le cas *CD25*, toutes égales à *0.50* dans le cas *CD50*, toutes égales à *0.75* dans le cas *CD75*, et toutes égales à *1.00* dans le cas *CD100* (les autodiagnostics sont alors parfaits, c'est-à-dire que toutes les défaillances sont détectées). Les résultats ont été obtenus d'après *500* simulations de Monte Carlo pour chacune de ces vingt configurations possibles, permettant alors de donner des résultats dont l'intervalle de confiance à *90*% est estimé à plus ou moins *3*% autour de la valeur moyenne. Les valeurs moyennes obtenues pour chaque configuration sont décrites sur la Figure IV.2.4.

D'après les résultats de la Figure IV.2.4, les remarques suivantes peuvent être faites :

- l'*algorithme de secours* augmente globalement la disponibilité du SCC, mais diminue sa sécurité, et ces écarts sont d'autant plus importants que les couvertures de diagnostic sont grandes ;
- l'*algorithme de contraste* augmente à la fois la disponibilité et la sécurité du SCC lorsque les couvertures de diagnostic sont très faibles, mais diminue ces deux critères lorsque les couvertures de diagnostic sont plus grandes.

Lorsque l'*algorithme de secours* est utilisé, un sous-système qui est diagnostiqué comme « *défaillant* » peut être fonctionnellement remplacé par un sous-système qui est diagnostiqué comme « *opérant* ». Cependant, un sous-système diagnostiqué comme « *opérant* » peut, en effet, être dans un état *opérant*, mais peut également être dans un état de *défaillance non détectée*. Ainsi, bien que l'*algorithme de secours* augmente la disponibilité du SCC (lorsqu'une fonction indisponible devient disponible), elle diminue aussi la sécurité (lorsqu'une fonction indisponible, diagnostiquée comme telle, reste indisponible, mais non diagnostiquée comme telle), et en particulier lorsque les couvertures de diagnostic sont faibles. Enfin, lorsque les couvertures de diagnostic sont assez grandes, l'utilisation de l'*algorithme de contraste* ne permet pas de produire un diagnostic qui soit meilleur que les résultats de diagnostic compilé obtenus à partir des autodiagnostics, et il n'est donc pas judicieux de remplacer ces derniers. Les recommandations suivantes peuvent alors être faites :

- l'utilisation de l'*algorithme de secours* doit être justifiée par les exigences de disponibilité et de sécurité qui se font alors concurrence ;
- l'utilisation de l'*algorithme de contraste* ne devrait être justifiée que si les couvertures de diagnostic sont très faibles, ou éventuellement si ces dernières sont un peu moins faibles mais à condition que l'*algorithme de secours* soit également utilisé.

IV.2.3.2. Conclusions partielles et perspectives

En utilisant des réseaux de Petri colorés et stochastiques, il a été possible de modéliser un SCC constitué de trois CTI, puis d'évaluer des critères de sûreté de fonctionnement d'après des simulations de Monte Carlo. Deux algorithmes ont été proposés afin d'améliorer la sûreté de fonctionnement du SCC en tirant avantage de la coopération entre ses CTI. D'après le pourcentage de temps que le SCC passe dans ses états fonctionnels au cours des *10 000* premières unités de temps, il a été montré que la disponibilité et la sécurité du SCC pouvaient être améliorées sous certaines conditions (notamment selon les couvertures de diagnostic des sous-systèmes des CTI) et, au minimum, être mis en balance par l'utilisation des algorithmes proposés.

En tant que principale conclusion, les résultats de cette étude donnent une indication sur l'implication des « fonctionnalités intelligentes » au sein des SCC. Lorsque ces « fonctionnalités intelligentes » sont utilisées de façon appropriées, elles permettent ainsi, en plus d'avantages pratiques, d'améliorer ou de mettre en balance certains critères de sûreté de fonctionnement.

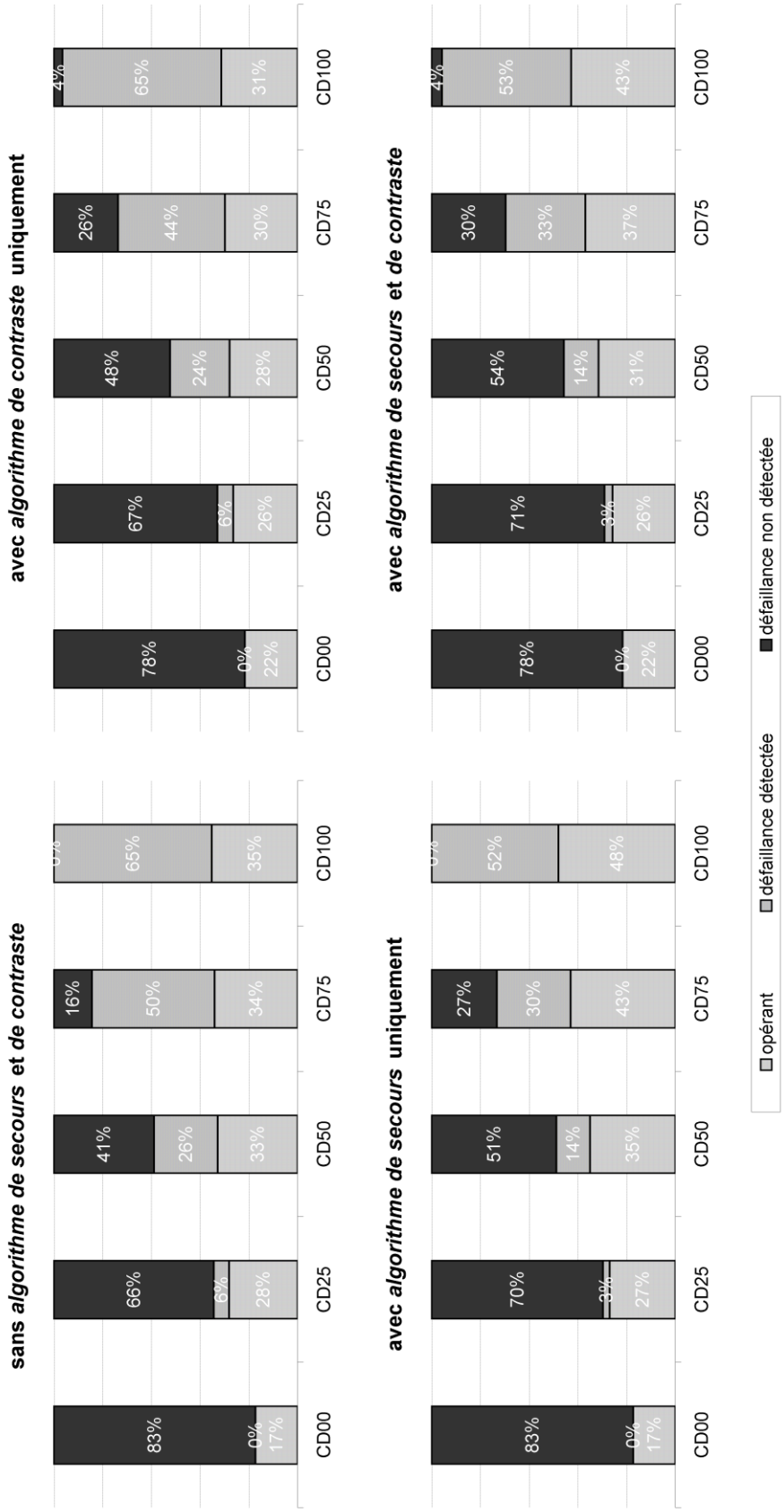

Figure IV.2.4. Résultats des évaluations du système de contrôle-commande (SCC)

Dans la Section IV.3, une modélisation et une évaluation d'un SCC intégrant des CTI est proposée en y intégrant à la fois les interactions entre les éléments du système (dont les CTI), ainsi qu'avec le processus contrôlé, dans une approche formalisée de fiabilité dynamique.

IV.3. FIABILITÉ DYNAMIQUE D'UN SYSTÈME DE CONTRÔLE-COMMANDE INTÉGRANT DES « CAPTEURS-TRANSMETTEURS INTELLIGENTS »

IV.3.1. Formalisation du Problème de Fiabilité Dynamique

IV.3.1.1. Formulation mathématique de la fiabilité dynamique

En plus du temps *t*, quatre types de variables sont utilisés pour définir l'état complet du système. Les variables d'état des composants et du processus sont les mêmes que celles définies par J. Devooght et C. Smidts [JDe92b] (cf. théorie des CET, Section IV.1.2). Des variables d'information sont, de plus, introduites afin de prendre en compte explicitement les particularités des CTI ; et des variables de déviation permettent d'étendre les possibilités de modélisation des défaillances. Toutes ces variables sont dépendantes du temps *t*. De plus, les variables d'état des composants sont de nature discrète et sont donc représentées par un vecteur d'entiers, noté $\boldsymbol{i(t)}$; les variables du processus, d'information, et de déviation, sont de nature continue et sont donc représentées par des vecteurs de réels, respectivement notés $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$. Le système ainsi défini est alors un « système hybride » (discret / continu). Les notations sont données dans le Tableau IV.3.1.

Les variables d'état des composants, données dans $\boldsymbol{i(t)}$, représentent la structure (configuration) du système selon les états physiques (par exemple, *opérants*, *dégradés*, *défaillants*) de ses composants et des actions humaines (par exemple, fermeture ou ouverture d'une vanne). L'état de chaque composant est décrit par un entier *n*, ou par un ensemble d'entiers (S_n), réunis dans le vecteur $\boldsymbol{i(t)}$, avec $\boldsymbol{i(t)} \in \mathbb{N}^N$. (Par exemple, un système composé de *N* composants, dont l'état de chacun d'eux est décrit par l'entier n_i tel que $n_i = 1$ si le composant *i* est *opérant* et $n_i = 0$ sinon, avec $i = 1, \ldots, N$, peut être décrit par le vecteur $\boldsymbol{i(t)} = (n_1, n_2, \ldots, n_N)^T$.) Les variables d'état des composants peuvent évoluer de façon déterministe ou stochastique, en fonction des variables du processus et d'information (par exemple, un actionneur est contrôlé par un signal i.e. une variable d'information, et a un taux de défaillance qui dépend de la température i.e. une variable du processus), et des variables de déviation (par exemple, après un certain degré de dégradation i.e. une variable de déviation, une transition d'un composant depuis un état *dégradé* vers un état de *défaillance totale* se produit). Le taux de transition des composants depuis l'état $\boldsymbol{i}^k$ vers l'état $\boldsymbol{i}^l$ au temps *t*, sachant les variables du processus, d'information, et de déviation ($\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$), est noté $p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$, (sur la base des notations introduites par la théorie des CET [JDe92b]). À noter que ces taux de transition peuvent prendre en compte des actions humaines (par exemple, lorsqu'un certain niveau de pression est détecté par l'intermédiaire d'un signal i.e. une variable d'information, un opérateur actionne une vanne i.e. un état de l'un des composants est modifié). Le taux de transition total des composants depuis l'état $\boldsymbol{i}^k$ est alors :

$$\lambda_{\boldsymbol{i}}{}^k(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) = \sum_{\boldsymbol{i}^l \neq \boldsymbol{i}^k} p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) \qquad \text{[IV.3.1]}$$

Les transitions entre deux états de composants sont considérées comme instantanées. Lorsque l'état des composants au temps *t* est $\boldsymbol{i(t)} = \boldsymbol{i}^k$, la probabilité pour que les composants quittent cet état avant l'instant $t + \tau$ est donc :

$$F_{\boldsymbol{i}}{}^k(\tau \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) = 1 - \exp\left(-\int_0^{\tau} \lambda_{\boldsymbol{i}}{}^k(\boldsymbol{x}(t+u), \boldsymbol{y}(t+u), \boldsymbol{e}(t+u), t+u) \cdot du \right) \qquad \text{[IV.3.2]}$$

Tableau IV.3.1. Nomenclature

paramètre	description
t_0	temps initial, avec $t_0 \in \mathbb{R}$ et $t_0 \geq 0$
t	variable temps, avec $t \in \mathbb{R}$ et $t \geq t_0$
N	nombre de variables d'état des composants, avec $N \in \mathbb{N}$
M	nombre de variables du processus, avec $M \in \mathbb{N}$
L	nombre de variables d'information, avec $L \in \mathbb{N}$
Q	nombre de variables de déviation, avec $Q \in \mathbb{N}$
$\boldsymbol{i(t)}$	vecteur des variables d'état des composants au temps t, avec $\boldsymbol{i(t)} \in \mathbb{N}^N$
$\boldsymbol{x(t)}$	vecteur des variables du processus au temps t, avec $\boldsymbol{x(t)} \in \mathbb{R}^M$
$\boldsymbol{y(t)}$	vecteur des variables d'information au temps t, avec $\boldsymbol{y(t)} \in \mathbb{R}^L$
$\bar{\boldsymbol{y}}\boldsymbol{(t)}$	vecteur des variables d'information au temps $t - \varepsilon$ i.e. $\bar{\boldsymbol{y}}\boldsymbol{(t)} = \boldsymbol{y(t - \varepsilon)}$ avec ε qui tend vers 0^+ (i.e. ε tend vers 0 avec $\varepsilon > 0$), avec $\bar{\boldsymbol{y}}\boldsymbol{(t)} \in \mathbb{R}^L$
$\boldsymbol{e(t)}$	vecteur des variables de déviation au temps t, avec $\boldsymbol{e(t)} \in \mathbb{R}^Q$
$p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$	taux de transition des composants depuis l'état $\boldsymbol{i}^k$ vers l'état $\boldsymbol{i}^l$ au temps t, sachant $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$
$\lambda_{\boldsymbol{i}^k}(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$	taux de transition total des composants depuis l'état $\boldsymbol{i}^k$ au temps t, sachant $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$
$F_{\boldsymbol{i}^k}(\tau \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$	probabilité pour les composants de quitter l'état $\boldsymbol{i}^k$ dans l'intervalle de temps $[t\ ;\ t + \tau]$, sachant $\boldsymbol{i(t)} = \boldsymbol{i}^k$, $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$
$\boldsymbol{[i]}$	vecteur des valeurs possibles du vecteur $\boldsymbol{i(t)}$, pour n'importe quel instant t i.e. chaque composante du vecteur $\boldsymbol{[i]}$ est une valeur possible du vecteur des variables d'état des composants
$E_{\boldsymbol{i}}$	nombre total de valeurs possibles du vecteur $\boldsymbol{i(t)}$ i.e. dimension du vecteur $\boldsymbol{[i]}$
$\boldsymbol{P}_{\boldsymbol{[i],i(t)}}(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)^T \cdot \boldsymbol{[i]}$	produit de vecteurs utilisé pour déterminer aléatoirement $\boldsymbol{i(t + \Delta t)}$ d'après les taux de transition, sachant $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$
$\boldsymbol{x'_{i(t)}(x(t), e(t), t)}$	vecteur des dérivées des variables du processus au temps t, sachant $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, et $\boldsymbol{e(t)}$, avec $\boldsymbol{x'_{i(t)}(x(t), e(t), t)} \in \mathbb{R}^M$

$\boldsymbol{y_{i(t)}(x(t), \bar{y}(t), e(t), t)}$	vecteur des variables d'information au temps t, sachant $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\boldsymbol{\bar{y}(t)}$, et $\boldsymbol{e(t)}$, avec $\boldsymbol{y_{i(t)}(x(t), \bar{y}(t), e(t), t)} \in \mathbb{R}^L$
$\boldsymbol{dE_{i(t)}(x(t), e(t), t, t + dt)}$	vecteur des incréments stochastiques du vecteur des variables de déviation dans l'intervalle de temps $[t ; t + dt]$, sachant $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, et $\boldsymbol{e(t)}$, avec $\boldsymbol{dE_{i(t)}(x(t), e(t), t, t + dt)} \in \mathbb{R}^Q$
$\boldsymbol{\xi_{dE_{i(t)}}(de, x(t), e(t), t, t + dt)}$	densité de probabilité de $\boldsymbol{dE_{i(t)}(x(t), e(t), t, t + dt)}$, en utilisant la variable d'intégration $\boldsymbol{de} \in \mathbb{R}^Q$, sachant $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, et $\boldsymbol{e(t)}$
$\boldsymbol{(i(t), x(t), y(t), e(t))}$	description de l'état complet du système au temps t
D	domaine de sécurité de l'état complet du système, généralement défini par une frontière Γ_x des variables du processus, telle que le système est dans un état *sûre* au temps t si et seulement si $\boldsymbol{x(t)} \leq \Gamma_x$
$\boldsymbol{v(t)}$	n'importe quel vecteur au temps t
$\boldsymbol{v(t)}_k$	$k^{\text{ème}}$ composante du vecteur $\boldsymbol{v(t)}$
$\boldsymbol{v}^k$	valeur spécifique du vecteur $\boldsymbol{v(t)}$, indicé par k
$\boldsymbol{[v]}$	vecteur des valeurs possibles du vecteur $\boldsymbol{v(t)}$, pour n'importe quel instant t i.e. $\boldsymbol{[v]}_k = \boldsymbol{v}^k$ pour $k = 1, \ldots, E_{\boldsymbol{v}}$ et $\boldsymbol{v}^k \neq \boldsymbol{v}^l$ pour $k \neq l$
$E_{\boldsymbol{v}}$	nombre total de valeurs possibles du vecteur $\boldsymbol{v(t)}$ i.e. dimension du vecteur $\boldsymbol{[v]}$
$\boldsymbol{[v]}_k$	$k^{\text{ème}}$ composante du vecteur $\boldsymbol{[v]}$ (avec $k = 1, \ldots, E_{\boldsymbol{v}}$)
$\boldsymbol{[v_k]}$	vecteur des valeurs possibles du vecteur $\boldsymbol{v(t)}_k$, pour n'importe quel instant t
$\boldsymbol{v}^k \pm \boldsymbol{\varepsilon_v}$	intervalle défini par $[\boldsymbol{v}^k - \boldsymbol{\varepsilon_v} ; \boldsymbol{v}^k + \boldsymbol{\varepsilon_v}]$
$\boldsymbol{v(t)}^T$	transposé du vecteur $\boldsymbol{v(t)}$
$\boldsymbol{v(t)}_{(S)}$	sous-ensemble (S) de composantes du vecteur $\boldsymbol{v(t)}$
$\boldsymbol{v(t)}_{(S),k}$	$k^{\text{ème}}$ composante du vecteur $\boldsymbol{v(t)}_{(S)}$
$\boldsymbol{v(t)}_{\setminus(S)}$	vecteur $\boldsymbol{v(t)}$ sans le sous-ensemble (S) de ses composantes
Δt	incrément de temps
$I_1(\text{A})$	fonction indicatrice définie par $I_1(\text{A}) = 1$ si l'assertion A est vraie, et $I_1(\text{A}) = 0$ sinon

Les variables du processus, données dans $\boldsymbol{x(t)}$, ($\boldsymbol{x(t)} \in \mathbb{R}^M$ avec M le nombre de variables du processus), représentent les variables physiques qui sont impliquées dans la dynamique du système (par exemple, pressions, températures, niveaux, volumes). Les variables du processus évoluent de façon déterministe, sachant l'état des composants, et avec les variables de déviation en tant que paramètres (par exemple, un niveau dans un réservoir est déterminé par la configuration des vannes i.e. une variable d'état des composants, et un degré de fuite i.e. une variable de déviation). Les évolutions des variables du processus peuvent alors généralement être définies par un ensemble d'équations différentielles (non-stochastiques) du premier ordre :

$$\frac{d}{dt}\,\boldsymbol{x(t)} = \boldsymbol{x'_{i(t)}(x(t), e(t), t)} \qquad \text{[IV.3.3]}$$

Les variables d'information, données dans $\boldsymbol{y(t)}$, ($\boldsymbol{y(t)} \in \mathbb{R}^L$ avec L le nombre de variables d'information), représentent les informations et les données qui sont traitées, calculées, stockées, et/ou échangées par/entre des composants du système (par exemple, signaux, résultats de mesure, informations de diagnostic). Par nature, les variables d'information n'affectent pas directement les variables du processus et de déviation, mais peuvent être utilisées pour modifier l'état des composants (par exemple, un signal commande l'activation d'une unité). Les variables d'information peuvent généralement être exprimées comme une fonction des variables du processus et de déviation, sachant l'état des composant (par exemple, lorsqu'un capteur est dans un état *dégradé* i.e. une variable d'état des composants, ses résultats de mesure dépendent de la grandeur mesurée i.e. une variable du processus, et de dérives i.e. des variables de déviation), et peuvent avoir pour origine des actions humaines (par exemple, une commande est transmise via une interface utilisateur). Elles peuvent aussi dépendre des précédentes valeurs des variables d'information (par exemple, un résultat est calculé à partir de données stockées, un signal est bloqué à une valeur courante) qui sont notées $\bar{\boldsymbol{y}}\boldsymbol{(t)}$, définies par $\bar{\boldsymbol{y}}\boldsymbol{(t)} = \boldsymbol{y(t - \varepsilon)}$ avec ε qui tend vers 0^+ (ε tend vers 0 avec $\varepsilon > 0$). Parce que le temps t figure explicitement en tant que paramètre, $\bar{\boldsymbol{y}}\boldsymbol{(t)}$ peut inclure des valeurs de variables d'information qui correspondent à n'importe quel instant jusqu'au temps t, en utilisant un nombre adéquat L de variables d'information (par exemple, une fonction peut être utilisée pour modifier des composantes de $\boldsymbol{y(t)}$ uniquement si le temps t rempli certaines conditions particulières). Finalement, les variables d'information sont exprimées par :

$$\boldsymbol{y(t)} = \boldsymbol{y_{i(t)}(x(t), \bar{y}(t), e(t), t)} \qquad \text{[IV.3.4]}$$

Les variables de déviation, données dans $\boldsymbol{e(t)}$, ($\boldsymbol{e(t)} \in \mathbb{R}^Q$ avec Q le nombre de variables de déviation), représentent les déviations ou les erreurs, de nature continue, dans les propriétés du système (par exemple, dégradations, dérives). Les variables de déviation évoluent de façon stochastique, sachant l'état des composants, et avec les variables du processus en tant que paramètres (par exemple, lorsqu'une vanne est fermée i.e. une variable d'état des composants, un niveau de fuite est une variable aléatoire distribuée selon une loi influencée par la pression i.e. une variable du processus). Un processus stochastique [SRo96] peut alors généralement être utilisé pour représenter les évolutions des variables de déviation, défini par un vecteur d'incréments stochastiques dans l'intervalle de temps $[t\,;\, t + dt]$:

$$\boldsymbol{e}(t + dt) = \boldsymbol{e(t)} + d\boldsymbol{E_{i(t)}(x(t), e(t)}, t, t + dt) \qquad \text{[IV.3.5]}$$

avec le vecteur stochastique $d\boldsymbol{E_{i(t)}(x(t), e(t)}, t, t + dt)$ dont la densité de probabilité est notée $\xi_{d\boldsymbol{E_{i(t)}}}\boldsymbol{(de, x(t), e(t)}, t, t + dt)$, ($\boldsymbol{de}$ est la variable d'intégration, utilisée pour représenter les réalisations de la variable aléatoire $d\boldsymbol{E_{i(t)}(x(t), e(t)}, t, t + dt)$).

Dans les Équations IV.3.3 à IV.3.5, qui définissent les variables de nature continue, l'état des composants figure en tant qu'indice. En effet, un jeu d'équations doit être théoriquement défini pour chaque état des composants (configuration du système). En pratique, une fonction indicatrice telle que $I_1(\text{A})$, définie par $I_1(\text{A}) = 1$ si l'assertion A est vraie, et $I_1(\text{A}) = 0$ sinon, peut, cependant, être

utilisée pour obtenir un seul jeu d'équations pour l'ensemble des variables continues. L'assertion A peut alors faire référence à l'état de l'ensemble des composants ou, le plus souvent, à seulement une partie des composants, donnée dans un sous-ensemble *(S)* de composantes du vecteur $\boldsymbol{i(t)}$, noté $\boldsymbol{i(t)}_{(S)}$. Dans les Équations IV.3.1 à IV.3.5, il est également possible d'y faire figurer explicitement un vecteur de paramètres, généralement noté $\boldsymbol{a}$ [JDe96, PLa00], qui est par exemple utilisé pour effectuer des analyses d'incertitudes [JDe98, JDe97].

L'état complet du système est alors décrit par l'ensemble $(\boldsymbol{i(t)}, \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)})$. Pour effectuer des analyses de risques, un domaine de sécurité, noté *D*, est alors défini de telle sorte que le système est considéré comme étant dans un état *sûr* si $(\boldsymbol{i(t)}, \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}) \in D$. Généralement, *D* ne fait référence qu'à des variables du processus, c'est-à-dire qu'un évènement dangereux est considéré si et seulement si certaines variables du processus (par exemple, une température, une pression) atteignent certaines valeurs. Le domaine *D* est alors défini par une frontière des variables du processus, notée $\Gamma_{\boldsymbol{x}}$, telle que l'état complet du système est *sûr* au temps *t* si et seulement si $\boldsymbol{x(t)} \leq \Gamma_{\boldsymbol{x}}$. Enfin, des analyses de fiabilité ont pour objectif d'évaluer la probabilité, en fonction du temps, que l'état complet du système quitte le domaine de sécurité, et plus généralement, des analyses de risques cherchent à étudier les scénarios correspondants.

IV.3.1.2. Solution numérique

Même sans variable d'information et de déviation, exprimer analytiquement la probabilité de l'état complet du système au temps *t* s'est montré impraticable, à l'exception de certains cas très simples [PLa96], et seules des solutions numériques ont été apportées [PLa96, CCo06a]. Des discussions sur les méthodes numériques applicables à ce type de problème peuvent être trouvées dans la littérature (par exemple, [REy08], [PNe07], [GSt09]). L'approche numérique adoptée dans ce présent travail est basée sur des développements de Taylor (afin de manipuler des taux de transition, cf. Équations IV.3.1 et IV.3.2) et des différences finies (afin, notamment, de manipuler des équations différentielles, cf. Équations IV.3.3).

Un incrément de temps, noté Δt, est introduit. Celui-ci doit être assez petit pour pouvoir considérer les variables $\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$, comme constantes dans tout intervalle $[t\ ;\ t + \Delta t]$, sans perdre en exactitude pour les analyses effectuées dans la suite. Ces variables au temps $t + \Delta t$ ($\boldsymbol{i(t + \Delta t)}$, $\boldsymbol{x(t + \Delta t)}$, $\boldsymbol{y(t + \Delta t)}$, et $\boldsymbol{e(t + \Delta t)}$) peuvent alors être déterminées d'après leurs valeurs au temps *t* ($\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$), en utilisant les Équations IV.3.1 à IV.3.5. En particulier, une transition des composants entre deux états qui se produit entre le temps *t* et le temps $t + \Delta t$ est considérée comme se produisant exactement au temps $t + \Delta t$. De même, les évolutions des variables du processus, d'information, et de déviation, entre les temps *t* et le temps $t + \Delta t$ sont considérées comme des « sauts » se produisant exactement au temps $t + \Delta t$.

Il est alors possible d'exprimer la probabilité que les composants restent dans leur état courant du temps *t*, noté $\boldsymbol{i(t)} = \boldsymbol{i}^k$, jusqu'au temps $t + \Delta t$, c'est-à-dire que $\boldsymbol{i(t + \Delta t)} = \boldsymbol{i}^k$, d'après l'Équation IV.3.2 et en utilisant un développement de Taylor (ici, le premier ordre de ce développement est utilisé, d'autres ordres peuvent également être exprimés dans le cas où l'incrément de temps Δt n'est pas assez petit pour permettre des approximations assez précises) :

$$P[\boldsymbol{i}(t + \Delta t) = \boldsymbol{i}^k \mid \boldsymbol{i(t)} = \boldsymbol{i}^k, \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t] = 1 - F_{\boldsymbol{i}}{}^k(\Delta t \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$$
$$\approx 1 - \Delta t \cdot \lambda_{\boldsymbol{i}}{}^k(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) \qquad \text{[IV.3.6]}$$

De même, la probabilité que les composants quittent leur état courant du temps t, noté $\boldsymbol{i(t) = i^k}$, pour un autre état en particulier au temps $t + \Delta t$, noté $\boldsymbol{i(t + \Delta t) = i^l}$, avec $\boldsymbol{i^k \neq i^l}$, peut être approximée par :

$$P[\boldsymbol{i(t + \Delta t) = i^l \neq i^k \mid i(t) = i^k, x(t), y(t), e(t)}, t] \approx \Delta t \cdot p(\boldsymbol{i^k \rightarrow i^l \mid x(t), y(t), e(t)}, t) \quad \text{[IV.3.7]}$$

À noter que des transitions déterministes (certaines) peuvent alors être modélisées par des taux de transition égaux à $1 / \Delta t$.

Pour déterminer l'état des composants au temps $t + \Delta t$, c'est-à-dire $\boldsymbol{i(t + \Delta t)}$, d'après les Équations IV.3.6 et IV.3.7, la procédure suivante peut être utilisée :

1. premièrement, des vecteurs sont définis afin de représenter toutes les valeurs possibles du vecteur des variables d'état des composants, et les probabilités de transition associées : soit $\boldsymbol{[i]}$ un vecteur défini par toutes les valeurs possibles du vecteur $\boldsymbol{i(t)}$, (pour n'importe quel instant t), c'est-à-dire que $\boldsymbol{[i]_k = i^k}$ pour $k = 1, \ldots, E_i$, ($\boldsymbol{[i]_k}$ est la $k^{\text{ème}}$ composante du vecteur $\boldsymbol{[i]}$), avec E_i le nombre total de valeurs possibles du vecteur $\boldsymbol{i(t)}$, et $\boldsymbol{i^k \neq i^l}$ pour $k \neq l$; et, sachant les variables de l'état complet du système au temps t ($\boldsymbol{i(t)}$, $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, et $\boldsymbol{e(t)}$), soit $\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)}$ un vecteur défini par les probabilités de transition depuis l'état $\boldsymbol{i(t)}$, c'est-à-dire que $\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)_k = \Delta t \cdot p(i(t) \rightarrow i^k \mid x(t), y(t), e(t), t)}$ si $\boldsymbol{i(t) \neq i^k}$, et $\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)_k = 1 - \Delta t \cdot \lambda_{i^k}(x(t), y(t), e(t), t)}$ si $\boldsymbol{i(t) = i^k}$, pour $k = 1, \ldots, E_i$, ($\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)_k}$ est la $k^{\text{ème}}$ composante du vecteur $\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)}$) ;
2. ensuite, la simulation de l'état des composants au temps $t + \Delta t$ ($\boldsymbol{i(t + \Delta t)}$) est obtenue par l'intermédiaire de deux variables aléatoires : soit $\boldsymbol{R_{[i],i(t)}(x(t), y(t), e(t), t)}$ une variable aléatoire (scalaire) discrète, d'espace des réalisations $(1, 2, \ldots, E_i)$, et de fonction de masse définie par $\boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)}$, c'est-à-dire que $P[\boldsymbol{R_{[i],i(t)}(x(t), y(t), e(t), t)} = k] = \boldsymbol{\rho_{[i],i(t)}(x(t), y(t), e(t), t)_k}$ pour $k = 1, \ldots, E_i$; et soit $\boldsymbol{P_{[i],i(t)}(x(t), y(t), e(t), t)}$ un vecteur dont toutes les composantes sont égales à 0, exceptée pour la composante indicée par la réalisation de $\boldsymbol{R_{[i],i(t)}(x(t), y(t), e(t), t)}$, qui est égale à 1 ;
3. enfin, $\boldsymbol{i(t + \Delta t) \approx P_{[i],i(t)}(x(t), y(t), e(t), t)^T \cdot [i]}$ [IV.3.8]

Les valeurs des variables du processus au temps $t + \Delta t$, c'est-à-dire $\boldsymbol{x(t + \Delta t)}$, peuvent être approximées d'après l'Équation IV.3.3, en utilisant des différences finies (avec $dt = \Delta t$) :

$$\boldsymbol{x(t + \Delta t) \approx x(t) + \Delta t \cdot x'_{i(t)}(x(t), e(t), t)} \quad \text{[IV.3.9]}$$

Les valeurs des variables de déviation au temps $t + \Delta t$, c'est-à-dire $\boldsymbol{e(t + \Delta t)}$, sont générées par des chemins du processus stochastique défini par l'Équation IV.3.5, en utilisant $dt = \Delta t$:

$$\boldsymbol{e(t + \Delta t) = e(t) + dE_{i(t)}(x(t), e(t), t, t + \Delta t)} \quad \text{[IV.3.10]}$$

Une fois les variables d'état des composants, du processus, et de déviation, définies au temps $t + \Delta t$, ($\boldsymbol{i(t + \Delta t)}$, $\boldsymbol{x(t + \Delta t)}$, et $\boldsymbol{e(t + \Delta t)}$), les variables d'information au temps $t + \Delta t$, c'est-à-dire $\boldsymbol{y(t + \Delta t)}$, peuvent être déterminées d'après l'Équation IV.3.4, avec $\varepsilon = \Delta t$ et $\bar{\boldsymbol{y}}\boldsymbol{(t + \Delta t) = y(t)}$:

$$\boldsymbol{y(t + \Delta t) \approx y_{i(t + \Delta t)}(x(t + \Delta t), y(t), e(t + \Delta t), t + \Delta t)} \quad \text{[IV.3.11]}$$

Les Équations IV.3.6 à IV.3.11 montrent que l'état complet du système au temps $t + \Delta t$, c'est-à-dire $\boldsymbol{(i(t + \Delta t), x(t + \Delta t), y(t + \Delta t), e(t + \Delta t))}$, peut être complètement déterminé d'après l'état complet du système au temps t, c'est-à-dire $\boldsymbol{(i(t), x(t), y(t), e(t))}$, selon des évolutions déterministes et stochastiques. Le système suit alors un processus (markovien) déterministe par morceau (PDP) [MDa84, MDA93].

Les développements suivants cherchent à exprimer la probabilité de l'état complet du système au temps $t + \Delta t$, d'après l'état complet du système au temps t. Parce que les Équations IV.3.9 à IV.3.11 fournissent des approximations numériques, les vecteurs (constants) suivants sont introduits : $\boldsymbol{\varepsilon_x}$

$\in \mathbb{R}^M$, $\boldsymbol{\varepsilon_y} \in \mathbb{R}^L$, et $\boldsymbol{\varepsilon_e} \in \mathbb{R}^Q$, afin d'exprimer l'état complet du système au temps t par $\boldsymbol{(i(t), x(t), y(t), e(t)) = (i^k, x^k \pm \varepsilon_x, y^k \pm \varepsilon_y, e^k \pm \varepsilon_e)}$, avec $\boldsymbol{v^k \pm \varepsilon_v}$ qui représente l'intervalle défini par $\boldsymbol{[v^k - \varepsilon_v ; v^k + \varepsilon_v]}$. De plus, les vecteurs $\boldsymbol{\varepsilon_x}$, $\boldsymbol{\varepsilon_y}$, et $\boldsymbol{\varepsilon_e}$, doivent être assez petits pour justifier l'approximation suivante :

$$\begin{aligned}&P[(\boldsymbol{i}(t+\Delta t), \boldsymbol{x}(t+\Delta t), \boldsymbol{y}(t+\Delta t), \boldsymbol{e}(t+\Delta t)) = (\boldsymbol{i}^k, \boldsymbol{x}^k \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}(t) \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}(t) \pm \boldsymbol{\varepsilon_e})\\ &| (\boldsymbol{i}(t), \boldsymbol{x}(t), \boldsymbol{y}(t), \boldsymbol{e}(t)) = (\boldsymbol{i}^l, \boldsymbol{x}^l \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}^l \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}^l \pm \boldsymbol{\varepsilon_e})]\\ &\approx P[(\boldsymbol{i}(t+\Delta t), \boldsymbol{x}(t+\Delta t), \boldsymbol{y}(t+\Delta t), \boldsymbol{e}(t+\Delta t)) = (\boldsymbol{i}^k, \boldsymbol{x}^k \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}(t) \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}(t) \pm \boldsymbol{\varepsilon_e})\\ &| (\boldsymbol{i}(t), \boldsymbol{x}(t), \boldsymbol{y}(t), \boldsymbol{e}(t)) = (\boldsymbol{i}^l, \boldsymbol{x}^l, \boldsymbol{y}^l, \boldsymbol{e}^l)]\end{aligned} \quad \text{[IV.3.12]}$$

pour tous états complets du système $\boldsymbol{(i^k, x^k, y^k, e^k)}$ et $\boldsymbol{(i^l, x^l, y^l, e^l)}$.

La probabilité conditionnelle de l'état complet du système au temps $t + \Delta t$, noté $\boldsymbol{(i(t+\Delta t), x(t+\Delta t), y(t+\Delta t), e(t+\Delta t)) = (i^k, x^k \pm \varepsilon_x, y^k \pm \varepsilon_y, e^k \pm \varepsilon_e)}$, sachant qu'il est dans un état particulier au temps t, noté $\boldsymbol{(i(t), x(t), y(t), e(t)) = (i^l, x^l, y^l, e^l)}$, peut alors être approximée par :

$$\begin{aligned}&P[(\boldsymbol{i}(t+\Delta t), \boldsymbol{x}(t+\Delta t), \boldsymbol{y}(t+\Delta t), \boldsymbol{e}(t+\Delta t)) = (\boldsymbol{i}^k, \boldsymbol{x}^k \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}(t) \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}(t) \pm \boldsymbol{\varepsilon_e})\\ &| (\boldsymbol{i}(t), \boldsymbol{x}(t), \boldsymbol{y}(t), \boldsymbol{e}(t)) = (\boldsymbol{i}^l, \boldsymbol{x}^l, \boldsymbol{y}^l, \boldsymbol{e}^l)]\\ &\approx [I_1(\boldsymbol{i}^l = \boldsymbol{i}^k) \cdot (1 - \Delta t \cdot \lambda_{\boldsymbol{i}^l}(\boldsymbol{x}^l, \boldsymbol{y}^l, \boldsymbol{e}^l, t)) + I_1(\boldsymbol{i}^l \neq \boldsymbol{i}^k) \cdot \Delta t \cdot p(\boldsymbol{i}^l \rightarrow \boldsymbol{i}^k \mid \boldsymbol{x}^l, \boldsymbol{y}^l, \boldsymbol{e}^l, t)]\\ &\cdot I_1(\boldsymbol{x}^k - \boldsymbol{\varepsilon_x} \leq \boldsymbol{x}^l + \Delta t \cdot \boldsymbol{x'}_{\boldsymbol{i}^l}(\boldsymbol{x}^l, \boldsymbol{e}^l, t) \leq \boldsymbol{x}^k + \boldsymbol{\varepsilon_x}) \cdot I_1(\boldsymbol{y}^k - \boldsymbol{\varepsilon_y} \leq \boldsymbol{y}_{\boldsymbol{i}^k}(\boldsymbol{x}^k, \boldsymbol{y}^l, \boldsymbol{e}^k, t + \Delta t) \leq \boldsymbol{y}^k + \boldsymbol{\varepsilon_y})\\ &\cdot 2 \cdot ||\boldsymbol{\varepsilon_e}|| \cdot \xi_{d\boldsymbol{E}_{\boldsymbol{i}^l}}(\boldsymbol{e}^k, \boldsymbol{x}^l, \boldsymbol{e}^l, t, t + \Delta t)\end{aligned} \quad \text{[IV.3.13]}$$

avec $I_1(A)$, la fonction indicatrice définie dans le Tableau IV.3.1, et $||\boldsymbol{\varepsilon_e}||$, la norme euclidienne du vecteur $\boldsymbol{\varepsilon_e}$.

La probabilité inconditionnelle de l'état complet du système au temps $t + \Delta t$, noté $\boldsymbol{(i(t+\Delta t), x(t+\Delta t), y(t+\Delta t), e(t+\Delta t)) = (i^k, x^k \pm \varepsilon_x, y^k \pm \varepsilon_y, e^k \pm \varepsilon_e)}$, peut quant à elle être approximé par :

$$\begin{aligned}&P[(\boldsymbol{i}(t+\Delta t), \boldsymbol{x}(t+\Delta t), \boldsymbol{y}(t+\Delta t), \boldsymbol{e}(t+\Delta t)) = (\boldsymbol{i}^k, \boldsymbol{x}^k \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}(t) \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}(t) \pm \boldsymbol{\varepsilon_e})]\\ &\approx \sum_{\boldsymbol{i}^l} \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} P[(\boldsymbol{i}(t+\Delta t), \boldsymbol{x}(t+\Delta t), \boldsymbol{y}(t+\Delta t), \boldsymbol{e}(t+\Delta t)) = (\boldsymbol{i}^k, \boldsymbol{x}^k \pm \boldsymbol{\varepsilon_x}, \boldsymbol{y}(t) \pm \boldsymbol{\varepsilon_y}, \boldsymbol{e}(t) \pm \boldsymbol{\varepsilon_e})\\ &| (\boldsymbol{i}(t), \boldsymbol{x}(t), \boldsymbol{y}(t), \boldsymbol{e}(t)) = (\boldsymbol{i}^l, \boldsymbol{x}^l, \boldsymbol{y}^l, \boldsymbol{e}^l)] \cdot d\boldsymbol{e}^l \cdot d\boldsymbol{y}^l \cdot d\boldsymbol{x}^l\end{aligned} \quad \text{[IV.3.14]}$$

Partant des conditions initiales au temps t_0, notées $\boldsymbol{(i(t_0), x(t_0), y(t_0), e(t_0))}$, il est ainsi possible d'évaluer la probabilité d'état complet du système au temps t, par une procédure d'itération basée sur les Équations IV.3.6 à IV.3.14. Les analyses de fiabilité cherchent alors à évaluer la probabilité suivante :

$$P[(\boldsymbol{i}(t), \boldsymbol{x}(t), \boldsymbol{y}(t), \boldsymbol{e}(t)) \in D] = P[\boldsymbol{x}(t) \leq \Gamma_{\boldsymbol{x}}] \quad \text{[IV.3.15]}$$

Il apparaît que le nombre scénarios possibles, d'après toutes les variables du système, peut être considérable. Dans la suite, une approche de Monte Carlo est donc adoptée pour calculer l'Équation IV.3.15 par itération des Équations IV.3.6 à IV.3.11. Contrairement à d'autres méthodes de Monte Carlo parmi les plus répandues, l'approche proposée ne simule pas les instants de temps où les variables sont modifiées, mais simule les évolutions des variables dans chaque incrément de temps Δt (les instants où les variables sont modifiées sont fixés et égaux à $t_0 + k \cdot \Delta t$ avec $k = 1, 2, \ldots$). Les évolutions des variables du système constituent alors des scénarios qui peuvent être classés selon leurs issues (par exemple, d'après des conditions sur des variables du processus). En répétant les simulations, la probabilité au temps t, définie par l'Équation IV.3.15, peut alors être évaluée par la fréquence relative d'occurrence de l'évènement $\{\boldsymbol{x}(t) \leq \Gamma_{\boldsymbol{x}}\}$. La prochaine section présente une approche générique permettant d'effectuer ces analyses de fiabilité en utilisant un formalisme basé sur des réseaux de Petri.

IV.3.2. Modélisation Formalisée en Réseaux de Petri

IV.3.2.1. Formalisme en réseau de Petri

D'une part, la fiabilité dynamique doit faire face à des transitions qui ont lieu à des instants de temps déterministes et stochastiques (conditionnées par le temps ou des variables du système), des évènements concurrents, et des transitions et séquences d'évènements simultanées [PLa00]. D'autre part, les réseaux de Petri fournissent des outils intéressants pour décrire et étudier des systèmes caractérisés comme étant concurrents, asynchrones, distribués, parallèles, non-déterministes, et/ou stochastiques [TMu89]. L'utilisation des réseaux de Petri pour la fiabilité dynamique est donc assez naturelle, et en particulier lorsqu'il est question de CTI. De plus, les réseaux de Petri colorés et stochastiques [FBa02b, JKe02] constituent des extensions prometteuses pour la modélisation de systèmes dynamiques [RDa94], notamment pour des analyses de risques [DVe03]. Par exemple, des réseaux de Petri stochastiques [YDu97b], et colorés [PSk08], ont déjà été exploités pour le problème de fiabilité dynamique « du réservoir » (cf. Section IV.1.2).

La théorie des réseaux de Petri est bien développée, et alimentée en permanence, comme le montre les nouvelles dénominations d'extensions qui apparaissent régulièrement dans la littérature. Plusieurs d'entre elles offrent des propriétés intéressantes pour prendre en compte des interactions entre des variables discrètes et continues : les réseaux de Petri hybrides [RDa10], qui permettent d'utiliser à la fois des nombres entiers et des réels pour marquer des places (« couleurs » de jetons) ; les réseaux de Petri colorés étendus [YYa95], qui modélisent des « changements de couleur » des jetons ; et des réseaux de Petri colorés dynamiques [MEv97], qui font explicitement le lien entre les réseaux de Petri et les PDP. Le calcul des équations différentielles peut aussi bénéficier des réseaux de Petri hybrides « hiérarchiques » [AGi96], et des réseaux de Petri « différentiels » [IDe98]. Un autre avantage des réseaux de Petri est qu'il existe un grand nombre d'outils logiciels disponibles [Pet10], dont certains sont gratuits et de bonne qualité.

Ce présent travail n'a pas pour objet de proposer une extension supplémentaire des réseaux de Petri. Les propriétés colorées et stochastiques sont ici considérées comme les deux aspects généraux utiles aux problèmes de fiabilité dynamique. La façon d'utiliser ces concepts doit, cependant, être définie dans l'optique de maximiser à la fois les capacités de modélisation et d'analyses. Un formalisme en réseau de Petri est donc présenté, qui utilise à la fois des propriétés colorées et stochastiques, afin de disposer d'une approche générique permettant de :

- modéliser de façon flexible la fiabilité dynamique d'un système, avec l'aide d'une interface qui soit visuelle et facile à manipuler ;
- simuler les évolutions de l'état complet du système, et effectuer des analyses de fiabilité correspondantes, en utilisant des méthodes numériques et des simulations de Monte Carlo.

Dans l'approche proposée, chaque place du réseau de Petri est associée à une ou à un ensemble de variables, et vice-versa. Le nombre de places est ainsi linéairement dépendant du nombre de variables, ce qui permet d'éviter les explosions combinatoires lors de la modélisation. Selon la nature des variables (discrète ou continue, déterministe ou stochastique), différentes représentations graphiques sont utilisées pour des raisons de convenance, telles que décrites sur la Figure IV.3.1. Les valeurs des variables sont données par les jetons (colorés), à l'aide de nombres réels ou entiers (selon les places) à l'intérieur des places correspondantes, et sont modifiées par les transitions. Chaque place contient ainsi en permanence un et un seul jeton et, par conséquent, toutes les transitions sont constamment franchissables. Des gardes sont donc utilisées pour chaque transition, et notées $s_j[\Delta t]$, ce qui signifie que la transition est franchie à chaque instant $s_j + k \cdot \Delta t$, avec $k = 0, 1, 2, \ldots$. De plus, les valeurs spécifiées sur les arcs (lorsque ces dernières sont nécessaires) ne font pas référence à un nombre de jetons, mais aux valeurs des variables manipulées.

Chaque transition du réseau de Petri est associée à une place particulière, nommée « place manipulée ». Cette place est liée à la transition par un arc d'entrée, ce qui signifie que les variables représentées par cette place sont modifiées par la transition (le jeton est « retiré » de la place) ; et liée à la même transition par un arc de sortie, qui attribue aux variables de sortie leurs nouvelles valeurs définie par l'expression spécifiée (un nouveau jeton est « déposé » dans la place). L'expression ainsi utilisée peut être une fonction des précédentes valeurs des variables (manipulées par l'arc d'entrée), ainsi que de variables représentées par d'autres places. Ces dernières places sont nommées les « places de dépendance » et sont liées à la transition par des arcs bidirectionnels, ce qui signifie que leurs variables peuvent être utilisées par la transition, mais ne sont pas modifiées. Les arcs d'entrée (des « places manipulées » vers leurs transitions associés) et les arcs bidirectionnels (entre les transitions et leurs « places de dépendance ») n'ont ainsi pas besoin d'être « valuées », car font toujours référence aux valeurs courantes des variables représentées par les places correspondantes. En revanche, les arcs de sortie (des transitions vers leurs « places manipulées ») doivent préciser les valeurs à attribuer, lors de chaque sollicitation, aux variables des « places manipulées ». Selon la « place manipulée » considérée, ces valeurs peuvent être des variables aléatoires. Contrairement aux approches plus « classiques » de réseaux de Petri stochastiques, les aspects stochastiques ne font ainsi pas référence aux instants de transition, mais à des valeurs de variables (la « couleur » des jetons). Le temps, en tant que variable, est également représenté par une place. En outre, toutes les transitions sont franchies à des instants déterministes (définies par les gardes des transitions). Ces réseaux de Petri peuvent ainsi être qualifiés de « réseaux de Petri (colorés et) stochastiques non-temporisés ».

Un réseau de Petri générique pour la modélisation de la fiabilité dynamique des systèmes est décrit sur la Figure IV.3.2, en utilisant les éléments décrits sur la Figure IV.3.1. Les cinq types de variables définis dans la Section IV.3.1 y sont modélisés, et représentés par différentes sortes de places. Sur la Figure IV.3.2, les variables sont données sous forme de vecteurs (excepté pour le temps t qui est un scalaire). Pour un modèle plus détaillé, et afin de traiter plus efficacement les dépendances entre variables, il est également possible de décomposer les vecteurs en sous-ensembles, avec une place pour chacun d'eux, et de les manipuler séparément (cf. l'exemple du CTI présenté dans la Section IV.3.2.2). Chaque transition est franchie à chaque incrément de temps Δt, modifiant les variables de la « place manipulée » correspondante, d'après les équations présentées dans la Section IV.3.1.2 et spécifiées par les arcs de sortie. Par exemple, la transition qui modifie la variable du temps t n'est liée à aucune « place de dépendance » et est simplement utilisée pour incrémenter le temps t par Δt lors de chaque transition. D'autre part, les variables de l'état des composants $\boldsymbol{i(t)}$ sont modifiées par des variables aléatoires qui dépendent de toutes les autres variables.

Dans chaque intervalle de temps $[t\ ;\ t + \Delta t]$, toutes les valeurs des variables au temps $t + \Delta t$ sont calculées suivant un ordre défini par les s_j (cf. partie supérieure de la Figure IV.3.2), et en utilisant les valeurs des variables au temps t, d'après les équations données dans la Section IV.3.1.2. En particulier, $\boldsymbol{x}(t + \Delta t)$ et $\boldsymbol{e}(t + \Delta t)$ dépendent tous deux de $\boldsymbol{x(t)}$ et $\boldsymbol{e(t)}$. Ainsi, pour éviter de « perdre » les valeurs de $\boldsymbol{x(t)}$, (respectivement, $\boldsymbol{e(t)}$), après le calcul de $\boldsymbol{x}(t + \Delta t)$, (respectivement, $\boldsymbol{e}(t + \Delta t)$), des méta-transitions sont introduites, telles que décrites sur la Figure IV.3.3. Celles-ci sont utilisées pour calculer les évolutions des variables dans l'intervalle de temps $[t\ ;\ t + \Delta t]$, ($\boldsymbol{x'_{i(t)}(x(t), e(t), t)}$ et $d\boldsymbol{E_{i(t)}(x(t), e(t), t, t + \Delta t)}$), les stocker en tant que variables additionnelles, puis modifier seulement après les variables du système. Une méta-transition a donc une double gardes, notée $(s_j, s_k)[\Delta t]$, ce qui signifie que les évolutions des variables sont calculées à chaque instant $s_j + k \cdot \Delta t$, et les variables des « places manipulées » à chaque instant $s_k + k \cdot \Delta t$, avec $k = 0, 1, 2, \ldots$ et $s_j < s_k$ (cf.

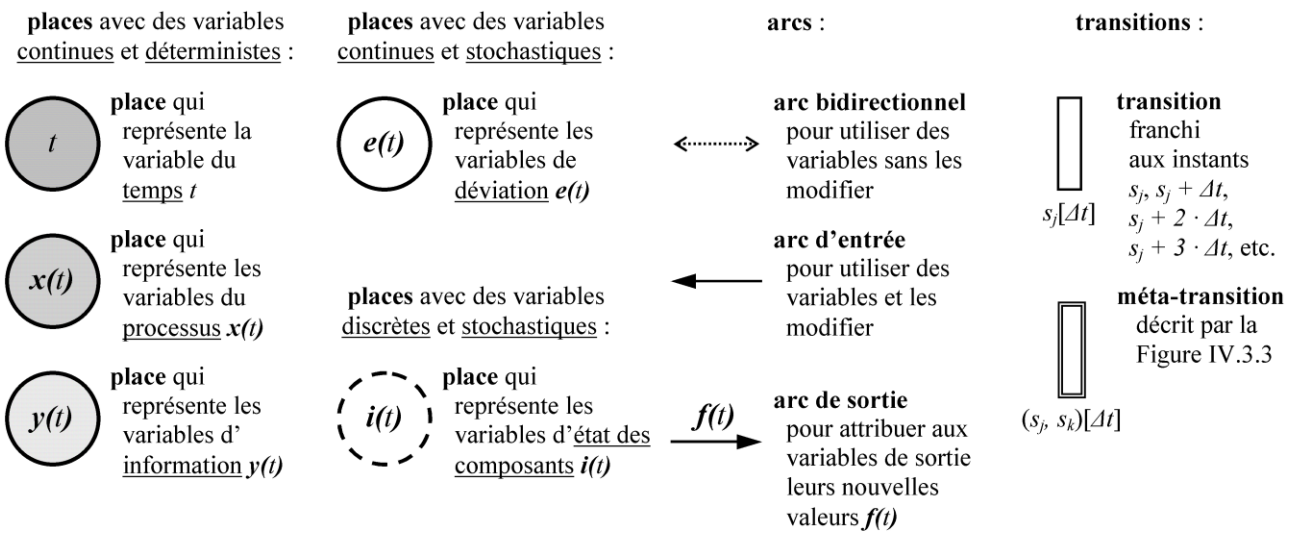

Figure IV.3.1. Éléments du réseau de Petri formalisé

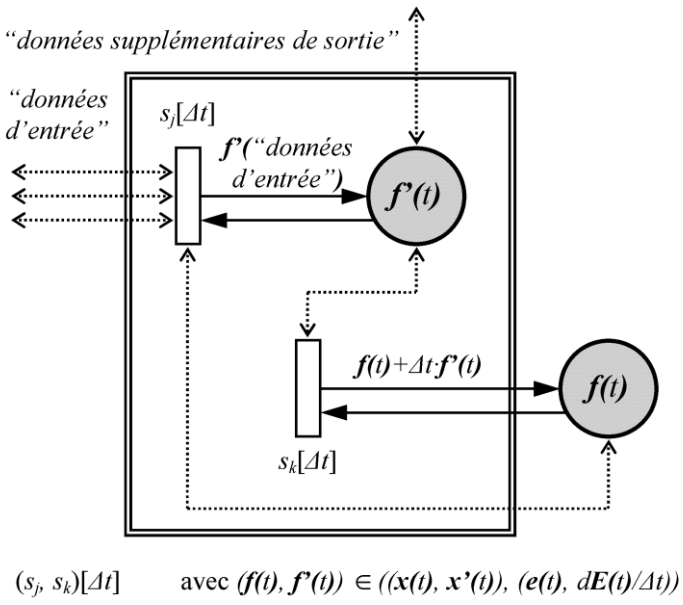

Figure IV.3.3. Méta-transition pour le réseau de Petri formalisé

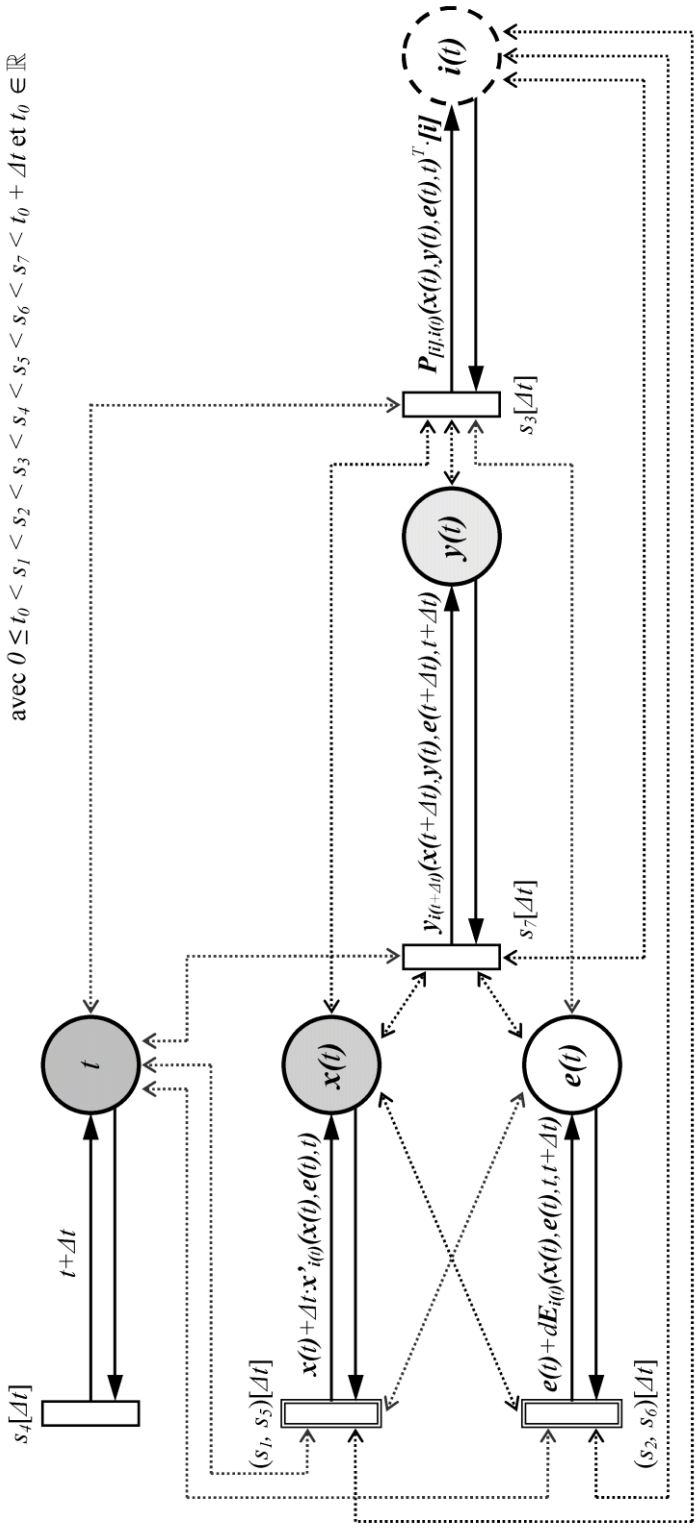

Figure IV.3.2. Réseau de Petri générique pour la modélisation de la fiabilité dynamique des systèmes

Figures IV.3.2 et IV.3.3). Pour s'assurer que les Équations IV.3.6 à IV.3.11 soient bien calculées, un ordre spécifique pour les s_j est requis (cf. partie supérieure de la Figure IV.3.2) : les évolutions des variables du processus et de déviation sont calculées en premier (d'après s_1 et s_2), parce qu'elles ne modifient pas les variables requises par les autres équations ; ensuite, les variables d'état des composants (d'après s_3), parce qu'elles nécessitent toutes les autres variables à l'instant courant ; la variable du temps t (d'après s_4) ; les variables du processus et de déviation (d'après s_5 et s_6), parce qu'elles ne dépendent maintenant plus que de leurs valeurs courantes et de leurs évolutions précédemment calculées (cf. Équations IV.3.9 et IV.3.10)) ; et finalement, les variables d'information (d'après s_7), parce qu'elles nécessitent toutes les autres variables au prochain instant de temps (cf. Équation IV.3.11). Afin de prendre en compte efficacement les dépendances entre sous-ensembles de variables, de tels ordonnancements peuvent aussi être requis parmi des variables de même type (lorsqu'elles sont modélisées séparément). De plus, les méta-transitions rendent disponibles des variables supplémentaires (les évolutions des variables du processus et d'information) qui peuvent, par exemple, faciliter certaines modélisations lorsque des évolutions de variables dépendent des dérivées d'autres variables.

IV.3.2.2. Modélisation des CTI

Un modèle générique pour la fiabilité dynamique des CTI est décrit sur la Figure IV.3.4, suivant le formalisme présenté dans la Section IV.3.2.1. Afin de rendre le modèle plus lisible, la place qui représente la variable du temps t est omise car elle peut potentiellement être liée à la plupart des autres places par des arcs bidirectionnels. Les spécifications des arcs de sortie ainsi que les gardes des transitions ne sont pas non plus représentées, car ces considérations ne relèvent pas d'un modèle générique. En revanche, l'attention est portée sur les variables d'information qui sont utilisées pour représenter les informations et les données qui sont manipulées par le CTI, et échangées entre le CTI et les autres éléments de systèmes (qui peuvent par exemple inclure d'autres CTI). Des sous-ensembles de variables d'information, issues du vecteur $\boldsymbol{y(t)}$, sont définis par des indices entre parenthèses (cf. Figure IV.3.4). Par exemple, $\boldsymbol{y(t)_{(T)}}$ contient toutes les variables d'information qui peuvent être modifiées par le CTI, et est lui-même composé de sous-ensembles expliqués ci-après. À l'inverse, $\boldsymbol{y(t)_{\setminus(T)}}$ contient toutes les autres variables d'information, ce qui inclut les informations et les données reçues d'autres éléments du système et, par exemple, des commandes humaines. Le vecteur $\boldsymbol{x(t)}$ contient, en particulier, la grandeur à mesurer par le CTI (le mesurande) ; $\boldsymbol{i(t)_{(T)}}$ donne l'état fonctionnel (*opérant* ou de *défaillance*, *détecté* ou *non détecté* par autodiagnostic) du CTI ; et $\boldsymbol{e(t)_{(T)}}$ représente des déviations du CTI, comme par exemple des dérives.

En tant qu'information « centrale », se trouve les données de traitement du CTI ($\boldsymbol{y(t)_{(P)}}$). Elles représentent tous les paramètres qui sont calculés par le CTI afin de fournir toute sorte d'information sur son état fonctionnel. Ces données de traitement peuvent être directement obtenues à partir de l'état du CTI ($\boldsymbol{i(t)_{(T)}}$), par exemple si celui-ci est en *défaillance détectée* ; ainsi qu'en utilisant des informations issues d'autres éléments du système ($\boldsymbol{y(t)_{\setminus(T)}}$), comme par exemple des résultats de mesure et des informations de diagnostic d'autres CTI. Les résultats de mesure du CTI ($\boldsymbol{y(t)_{(M)}}$) peuvent également être exploités, par exemple pour les comparer avec des résultats d'autres CTI. Enfin, certaines données peuvent être stockées ($\boldsymbol{y(t)_{(D)}}$), par exemple pour évaluer la cohérence des informations courantes avec les résultats précédents.

En utilisant les données de traitement, si l'état du CTI est jugé « inapproprié », des reconfigurations peuvent être commandées ($\boldsymbol{y(t)_{(R)}}$), par exemple pour activer une redondance passive au sein du CTI (reconfiguration fonctionnelle), ou pour modifier une bande de mesure (reconfiguration métrologique).

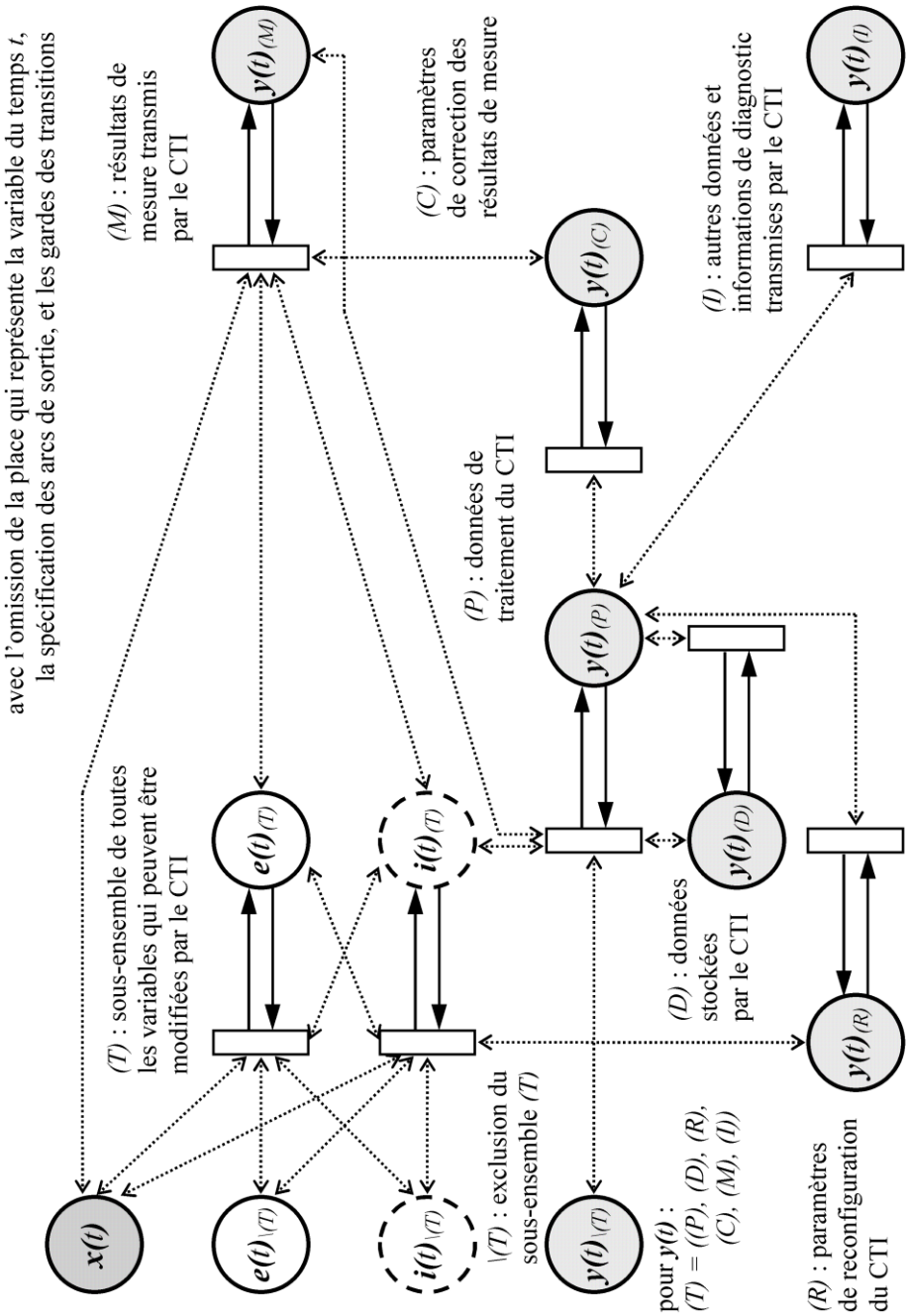

Figure IV.3.4. Réseau de Petri générique pour la modélisation de la fiabilité dynamique des « capteurs-transmetteurs intelligents » (CTI)

Les résultats de mesure du CTI ($\boldsymbol{y(t)_{(M)}}$) sont alors fonction de l'état du CTI ($\boldsymbol{i(t)_{(T)}}$), de la grandeur à mesurer (incluse dans $\boldsymbol{x(t)}$), et de possibles erreurs comme des dérives ($\boldsymbol{e(t)_{(T)}}$). De plus, des paramètres de correction ($\boldsymbol{y(t)_{(C)}}$), définis à partir des données de traitement, peuvent, par exemple, permettre de corriger certaines dérives.

En plus des résultats de mesure, le CTI est aussi capable de transmettre d'autres données telles que des informations de diagnostic ($\boldsymbol{y(t)_{(I)}}$) à d'autres éléments du système, comme par exemple un degré de confiance dans les résultats.

En fonction de la spécificité des applications, d'autres relations entre les éléments de la Figure IV.3.4 (définies par des arcs bidirectionnels) peuvent être ajoutées. Par exemple, les données stockées, les résultats de mesure, et les données issues d'autres éléments du système (respectivement, $\boldsymbol{y(t)_{(D)}}$, $\boldsymbol{y(t)_{(M)}}$, et $\boldsymbol{y(t)_{\backslash(T)}}$) peuvent, dans certains cas, être exploitées uniquement par l'intermédiaire des données de traitement (hypothèses faite sur la Figure IV.3.4), ou bien être directement utilisées pour les calculs des autres variables (un tel exemple est donné par le cas d'étude présenté dans la Section IV.3.3).

IV.3.3. Cas d'Étude : Système de Sécurité pour Réacteur Nucléaire

IV.3.3.1. Description du cas d'étude

IV.3.3.1.1. Réacteur nucléaire rapide Europa

Le cas d'étude développé dans cette section est un extrait du circuit primaire du réacteur nucléaire rapide Europa. Ce système a notamment été proposé comme support de référence pour des analyses de séquences d'évènements accidentelles [CEC89]. Plusieurs analyses de fiabilité ont également été effectuées sur cette application, en utilisant DYLAM [AAm84], des méthodes de Monte Carlo [CSm92], et une approche par ESD [SSw00] (cf. Section IV.1.2). Une description très complète du système original a été donnée par C. Smidts et J. Devooght [CSm92]. Dans ce présent travail, les variables physiques ont été simplifiées (les effets de la radioactivité en conditions nominales d'opération ont été négligées, en accord avec de précédents travaux qui ont montré l'impact marginal de la réactivité sur les fonctions de sécurité [SSw00]), pour mieux se concentrer sur d'autres aspects. En particulier, de nouvelles fonctionnalités des capteurs-transmetteurs ont été introduites (traitements de données, communications bidirectionnelles, corrections des erreurs de mesure), ainsi que des variables de déviation. Quelques notations, ainsi que des valeurs de taux de défaillance, ont aussi été modifiées par rapport au système original.

Le schéma simplifié du circuit primaire du réacteur Europa est décrit sur la Figure IV.3.5. Ce système comprend deux canaux (C1 et C2), où du sodium est introduit, en tant que réfrigérant, par une pompe (PM). Le manque de réfrigérant, par exemple en cas d'une défaillance de la pompe, entraîne une augmentation de la température à l'intérieur des canaux et peut causer des accidents. La fonction de sécurité étudiée dans la suite consiste donc à détecter un seuil haut de température dans les canaux, ou un seuil bas du flux de sodium, pour activer un système d'arrêt d'urgence. La température du sodium dans chaque canal (respectivement, T_1 et T_2) est donc mesurée par un capteur-transmetteur (respectivement, ST1 et ST2), qui transmet ses résultats de mesure (respectivement, T_1^m et T_2^m) à un contrôleur commun (CT). De même, le flux (taux de flux en quantité de mouvement) de sodium (G) est mesuré par un troisième capteur-transmetteur (SG), qui

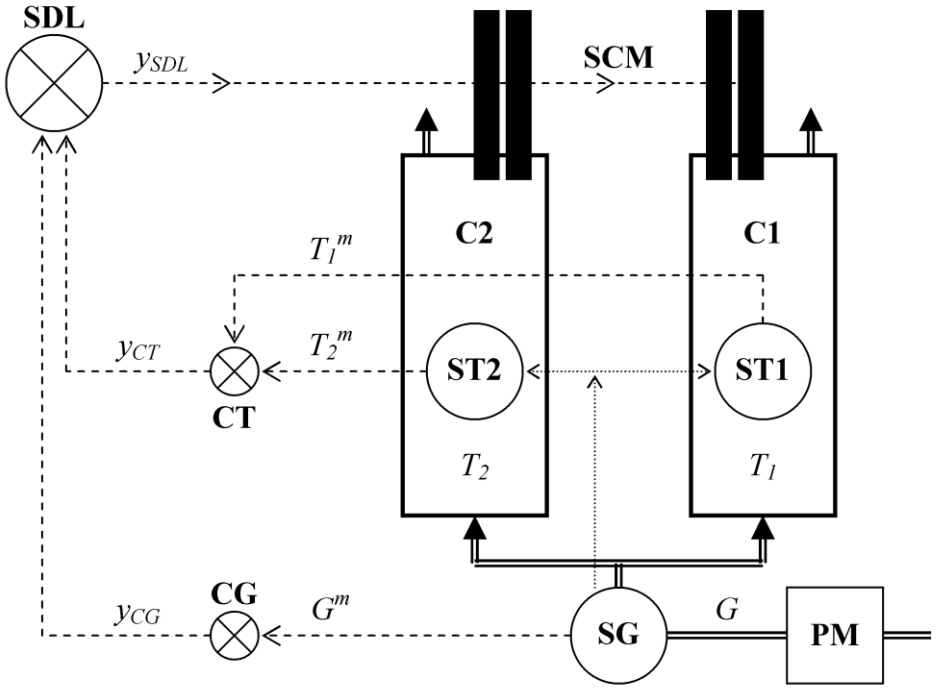

Figure IV.3.5. Schéma simplifié du circuit primaire du réacteur nucléaire rapide Europa

transmet ses résultats de mesure (G^m) à un contrôleur dédié (CG). Les deux contrôleurs primaires (CT et CG) envoient des signaux binaires (respectivement, y_{CT} et y_{CG}) à une unité centrale de contrôle (SDL). Si un seuil haut de température (T_{max}) est détecté dans au moins un des canaux ($y_{CT} = 1$), ou un seuil bas du flux sodium ($y_{CG} = 1$) en sortie de la pompe, alors l'unité centrale de contrôle envoie un signal binaire (y_{SDL}) qui doit activer un arrêt d'urgence (SCM), ($y_{SDL} = 1$). Cet équipement de sécurité, couramment nommé SCRAM, consiste à insérer, sous l'effet de la gravité, des barres de contrôle à l'intérieur du cœur du réacteur, ce qui a pour effet de stopper rapidement la réaction nucléaire par absorption des neutrons.

La description complète des variables du système (variables d'état des composants, du processus, d'information, et de déviation) est donnée dans les sections suivantes. Préliminairement, il convient de préciser que la pompe (PM) peut être dans un état de *défaillance totale*, ce qui implique un flux de sodium nul, ou bien sujette à des déviations de son couple (notées δ_M), ce qui implique un flux de sodium décroissant. De plus, les capteurs-transmetteurs de température (ST1 et ST2) peuvent être sujets à des dérives (respectivement notées δ_{D1} et δ_{D2}), ce qui implique des résultats de mesure (respectivement, T_1^m et T_2^m) qui sont aléatoirement biaisés. Des « fonctionnalités intelligentes » des capteurs-transmetteurs sont alors utilisées pour effectuer des corrections d'erreurs de mesure (biais dus aux dérives). Pour cela, les trois capteurs-transmetteurs (ST1, ST2, et SG) sont capables de stocker, échanger, et traiter des données, dans le but de détecter de potentielles dérives, et d'introduire des paramètres de correction (notés T_1^c et T_2^c) dans leurs résultats de mesure.

IV.3.3.1.2. Variables d'état des composants

Huit composants (éléments) du système sont considérés : deux composants mécaniques qui sont la pompe et le SCRAM (PM et SCM), trois capteurs-transmetteurs (SG, ST1, et ST2), et trois contrôleurs (CG, CT, et SDL). L'état de chacun de ces composants est représenté par un nombre entier fini, tel que défini dans le Tableau IV.3.2. Le vecteur des variables d'état des composants au temps t est donc $\boldsymbol{i(t)} = \boldsymbol{(}SPM(t), SSG(t), SCG(t), SST1(t), SST2(t), SCT(t), SSDL(t), SSCM(t)\boldsymbol{)}^T$ et $\boldsymbol{i(t)} \in \mathbb{N}^N$ avec $N = 8$. Dans la suite, et en accord avec le formalisme présenté dans la Section IV.3.2.1, chaque composante du vecteur $\boldsymbol{i(t)}$, (l'état d'un des composants), est modélisée séparément.

L'état *opérant* (fonctionnement nominal) d'un composant est représenté par une variable d'état qui est égale à *1* : lorsque $SPM(t) = 1$, la pompe réalise sa fonction avec des performances nominales ; lorsque $SSCM(t) = 1$, le SCRAM n'est pas activé mais est capable de l'être sur demande ; lorsque $SSG(t) = 1$, $SST1(t) = 1$, et $SST2(t) = 1$, les capteurs-transmetteurs transmettent des résultats de mesure qui sont corrects (ni bloqués, ni sujets à des dérives) ; et lorsque $SCG(t) = 1$, $SCT(t) = 1$, et $SSDL(t) = 1$, les contrôleurs envoient des signaux corrects. Lorsque la variable d'état d'un composant est égale à *0*, l'état correspondant est une *défaillance dangereuse*, c'est-à-dire qu'elle peut directement impliquer l'occurrence d'un évènement dangereux ou rendre indisponible la fonction de sécurité : les composants mécaniques ne sont plus capables d'assurer leurs fonctions ; les résultats de mesure des capteurs-transmetteurs sont bloqués à leurs valeurs courantes (et donc, ils ne sont plus capables de détecter le dépassement d'un nouveau seuil) ; et les signaux des contrôleurs sont bloqués aux valeurs *0* (signaux qui ne commandent pas l'activation du SCRAM). Au contraire, lorsque la variable d'état d'un composant est égale à *2*, l'état correspondant est une *défaillance sûre*, c'est-à-dire qu'elle peut directement impliquer une activation intempestive du SCRAM (activation du SCRAM alors que les températures et le flux de sodium n'ont pas dépassés les valeurs seuils) : les résultats de mesure des capteurs-transmetteurs sont bloqués à des valeurs qui sont soit égales, soit au-delà (pour la température) ou en deçà (pour le flux) des valeurs seuils ; les signaux des contrôleurs sont bloqués aux valeurs *1* (signaux qui commandent l'activation du SCRAM). Des états de *défaillance sûre* ne sont pas considérés pour les composants mécaniques.

D'autres valeurs de variables d'état des composants, égales à *3* ou à *4*, correspondent à des états *dégradés* (qui incluent des états de *dérives*) : le couple de la pompe est sujet à des déviations ; les résultats de mesure des capteurs-transmetteurs de température sont sujets à des dérives positives ou négatives (respectivement, surestimation et sous-estimation des grandeurs mesurées). Des états *dégradés* ne sont pas considérés pour les autres composants. Enfin, l'*activation* du SCRAM correspond à un état spécifique, qui est traduit par une variable d'état du SCRAM égale à *5*.

Les variables d'état des composants mécaniques affectent directement les variables du processus telles que décrites dans la Section IV.3.3.1.3. D'autre part, les variables d'état des capteurs-transmetteurs et des contrôleurs déterminent directement les variables d'information telles que décrites dans la Section IV.3.3.1.4. Enfin, les effets des états *dégradés* sont modélisés en utilisant des variables de déviation telles que décrites dans la Section IV.3.3.1.5.

Les taux de transition entre les états possibles de chaque composant sont donnés dans le Tableau IV.3.3. À noter que certains taux de transitions dépendent directement du temps *t* (un taux de transition du SCRAM correspond à une distribution de Weibull avec un paramètre de forme égal à *2.0*, un paramètre d'échelle égal à *8 000* secondes, hors effet des température, et à un paramètre de localisation égal au temps initial t_0), de variables du processus (des taux de transition des capteurs-transmetteurs de température et du SCRAM sont fonction des températures $T_1(t)$ et $T_2(t)$), de variables de déviation (un taux de transition de la pompe est fonction des déviations $\delta_M(t)$ du couple de celle-ci), de variables d'information (pour l'activation du SCRAM, en fonction du signal de l'unité centrale de contrôle, $y_{SDL}(t)$), ainsi que des états d'autres composants (les états des capteurs-transmetteurs de température dépendent l'un de l'autre de façon stochastique, dû à des causes communes de défaillance). Enfin, une transition déterministe (certaine) est utilisée pour l'activation du SCRAM (depuis l'état $SSCM(t) = 1$ vers l'état $SSCM(t) = 5$), lorsque celui-ci est dans un état *opérant* et que l'unité centrale de contrôle envoie un signal égale à *1* ($y_{SDL}(t) = 1$). Cette transition est modélisée en utilisant un taux de transition qui tend vers l'infini, c'est-à-dire égal à $1 / \varepsilon$, avec ε qui tend vers 0^+. (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1 : $\varepsilon = \Delta t$.)

IV.3.3.1.3. Variables du processus

La dynamique des variables physiques du système est déterminée par treize variables du processus qui sont modélisées séparément et définies par des équations différentielles du premier ordre. Le vecteur des variables du processus au temps *t* est $\boldsymbol{x(t)} = (\omega(t), G(t), T_{c,1}(t), T_{c,2}(t), T_1(t), T_2(t), P(t), C_1(t), C_2(t), C_3(t), C_4(t), C_5(t), C_6(t))^T$, avec $\boldsymbol{x(t)} \in \mathbb{R}^M$ et $M = 13$. Les paramètres utilisés dans les définitions des variables du processus sont donnés dans le Tableau IV.3.4, ainsi que les conditions initiales au temps $t = t_0$, qui correspondent aux états stationnaires des variables du processus ($\boldsymbol{x(t)}$ est constant dans le temps si les états des composants sont *opérants* et que les variables de déviation sont nulles) sont donnés dans le Tableau IV.3.5.

La vitesse angulaire de la pompe, notée $\omega(t)$ [rad·s^{-1}], est donnée par :

$$\frac{d}{dt}\omega(t) = \frac{C_M \cdot I_1\left(SPM(t) \neq 0\right) - \delta_M(t) \cdot I_1\left(SPM(t) = 3\right) - K \cdot \omega(t)}{I} \qquad \text{[IV.3.16]}$$

avec $SPM(t)$, la variable d'état de la pompe, définie dans la Section IV.3.3.1.2 (cf. Tableau IV.3.2) ; $\delta_M(t)$, la variable de déviation du couple de la pompe, définie dans la Section IV.3.3.1.5 ; et $I_1(\text{A})$, la fonction indicatrice, définie dans le Tableau IV.3.1. Les autres paramètres sont donnés dans le Tableau IV.3.4.

Le flux de sodium (taux de flux en quantité de mouvement), noté $G(t)$ [kg·m^{-2}·s^{-1}], est donné par :

Tableau IV.3.2. Variables d'état des composants

composant	variable d'état	valeur	description
pompe (PM)	*SPM(t)*	*= 1*	*opérant* : le couple de la pompe est nominal
		= 0	*défaillance totale* : le couple de la pompe est nul
		= 3	*dégradé* : le couple est sujet à des déviations
capteur-transmetteur de flux (SG)	*SSG(t)*	*= 1*	*opérant* : les résultats de mesure sont corrects
		= 0	*défaillance dangereuse* : bloqués à la valeur courante
		= 2	*défaillance sûre* : bloqués à G_{min} ou en deçà
contrôleur de flux (CG)	*SCG(t)*	*= 1*	*opérant* : le signal est correct
		= 0	*défaillance dangereuse* : bloqué à la valeur *0*
		= 2	*défaillance sûre* : bloqué à la valeur *1*
capteur-transmetteur de température *i* (STi), avec *i = 1, 2*	*SSTi(t)*	*= 1*	*opérant* : les résultats de mesure sont corrects
		= 0	*défaillance dangereuse* : bloqués à la valeur courante
		= 2	*défaillance sûre* : bloqués à T_{max} ou au-delà
		= 3	*dérives dangereuses* : sujets à des dérives négatives
		= 4	*dérives sûres* : sujets à des dérives positives
contrôleur de température (CT)	*SCT(t)*	*= 1*	*opérant* : le signal est correct
		= 0	*défaillance dangereuse* : bloqué à la valeur *0*
		= 2	*défaillance sûre* : bloqué à la valeur *1*
unité centrale de contrôle (SDL)	*SSDL(t)*	*= 1*	*opérant* : le signal est correct
		= 0	*défaillance dangereuse* : bloqué à la valeur *0*
		= 2	*défaillance sûre* : bloqué à la valeur *1*
SCRAM (SCM)	*SSCM(t)*	*= 1*	*opérant* : le SCRAM peut être activé
		= 0	*défaillance totale* : le SCRAM ne peut pas être activé
		= 5	*activation* : le SCRAM est activé

Tableau IV.3.3. Taux de transition des composants

variable d'état	depuis l'état	vers l'état	taux de transition	valeur[a] [seconde^{-1}]
$SPM(t)$	1 ou 3	0	$\lambda_{PM,0}(\delta_M(t))$	$= 1{\cdot}10^{-3} \cdot exp(\delta_M(t) \cdot 5{\cdot}10^{-5})$
	1	3	$\lambda_{PM,3}$	$= 1{\cdot}10^{-2}$
$SSG(t)$	1	0	$\lambda_{SG,0}$	$= 2{\cdot}10^{-3}$
	1	2	$\lambda_{SG,2}$	$= 2{\cdot}10^{-4}$
$SCG(t)$	1	0 ou 2	$\lambda_{CG,0/2}$	$= 1{\cdot}10^{-5}$
$SST1(t)$	1, 3 ou 4	0	$\lambda_{ST1,0}(SST2(t), T_1(t))$	$= 4{\cdot}10^{-4} \cdot (1 + I_1(SST2(t) = 0)) \cdot r(T_1(t))$
	1, 3 ou 4	2	$\lambda_{ST1,2}(SST2(t), T_1(t))$	$= 4{\cdot}10^{-5} \cdot (1 + I_1(SST2(t) = 2)) \cdot r(T_1(t))$
	1	3 ou 4	$\lambda_{ST1,3/4}$	$= 1.5{\cdot}10^{-2}$
$SST2(t)$	1, 3 ou 4	0	$\lambda_{ST2,0}(SST1(t), T_2(t))$	$= 4{\cdot}10^{-4} \cdot (1 + I_1(SST1(t) = 0)) \cdot r(T_2(t))$
	1, 3 ou 4	2	$\lambda_{ST2,2}(SST1(t), T_2(t))$	$= 4{\cdot}10^{-5} \cdot (1 + I_1(SST1(t) = 2)) \cdot r(T_2(t))$
	1	3 ou 4	$\lambda_{ST2,3/4}$	$= 1.5{\cdot}10^{-2}$
$SCT(t)$	1	0 ou 2	$\lambda_{CT,0/2}$	$= 1{\cdot}10^{-5}$
$SSDL(t)$	1	0 ou 2	$\lambda_{SDL,0/2}$	$= 1{\cdot}10^{-6}$
$SSCM(t)$	1	0	$\lambda_{SCM,0}(T_1(t), T_2(t), t)$	$= 3.125{\cdot}10^{-8} \cdot (t - t_0) \cdot r((T_1(t) + T_2(t))/2)$
	1	5	$\lambda_{SCM,5}(y_{SDL}(t))$	$= I_1(y_{SDL}(t) = 1) \cdot (1 / \varepsilon)$[b]

[a]Avec la fonction indicatrice $I_1(A)$, définie dans le Tableau IV.3.1, et la fonction suivante, utilisée pour modéliser l'effet de la température sur les taux de transition : $r(T) = 6.17{\cdot}10^{-2} \cdot exp(5.21{\cdot}10^{-3} \cdot T)$.
[b]Avec le paramètre ε qui tend vers 0^+, de telle sorte que $\lambda_{SCM,5}$ tende vers l'infini (transition déterministe et certaine) lorsque $y_{SDL}(t) = 1$.

Tableau IV.3.4. Paramètres des variables du processus

paramètre	valeur	unité	description
C_M	$= 60\,000$	N·m	couple nominal de la pompe
K	$= 10$	$kg \cdot m^2 \cdot s^{-1}$	constante qui modélise des phénomènes de friction
I	$= 10$	$kg \cdot m^2$	moment d'inertie de la pompe
υ	$= -5.00 \cdot 10^{-2}$	s^{-1}	constante utilisée pour l'évolution du flux de sodium
C_{nt2}	$= 5.56 \cdot 10^{-6}$	$kg \cdot m^{-2}$	constante utilisée pour l'évolution du flux de sodium
R	$= 9.521 \cdot 10^{-7}$	$K \cdot W^{-1}$	résistance thermique
w_1	$= 0.41175$	.	proportion d'énergie générée par C1, avec $w_1 + w_2 = 1$
w_2	$= 0.58825$	.	proportion d'énergie générée par C2, avec $w_1 + w_2 = 1$
T_e	$= 653$	K	température critique du sodium dans le réacteur
$\tau_1(T)$	$= 1.1223 + 1.5215 \cdot 10^{-3} \cdot T - 1.0471 \cdot 10^{-6} \cdot T^2 + 2.7476 \cdot 10^{-10} \cdot T^3$	s	constante de temps qui prend en compte la température spécifique du combustible dans C1
$\tau_2(T)$	$= 1.5714 + 2.1303 \cdot 10^{-3} \cdot T - 1.4661 \cdot 10^{-6} \cdot T^2 + 3.8470 \cdot 10^{-10} \cdot T^3$	s	constante de temps qui prend en compte la température spécifique du combustible dans C2
A_1	$= 0.518867$	m^2	section de passage du sodium dans C1
A_2	$= 0.741238$	m^2	section de passage du sodium dans C2
$C_R(T)$	$= 1629 - 8.3290 \cdot 10^{-1} \cdot T$	$J \cdot kg^{-1} \cdot K^{-1}$	chaleur spécifique du sodium
γ_{SCM}	$= 4.40 \cdot 10^{-1}$	s^{-1}	réactivité induite par les barres de contrôle insérées dans le cœur du réacteur[a]
β_1	$= 8.2100 \cdot 10^{-5}$	.	fraction de neutrons différés
β_2	$= 7.4480 \cdot 10^{-4}$	.	fraction de neutrons différés
β_3	$= 6.6150 \cdot 10^{-4}$	.	fraction de neutrons différés
β_4	$= 1.3277 \cdot 10^{-3}$	.	fraction de neutrons différés
β_5	$= 6.1480 \cdot 10^{-4}$	.	fraction de neutrons différés
β_6	$= 1.8940 \cdot 10^{-4}$	.	fraction de neutrons différés
Γ	$= 3.98 \cdot 10^{-2}$	s	durée de vie moyenne de production des neutrons[a]
γ_1	$= 1.29 \cdot 10^{-2}$	s^{-1}	constante de désintégration des précurseurs[a]
γ_2	$= 3.11 \cdot 10^{-2}$	s^{-1}	constante de désintégration des précurseurs[a]
γ_3	$= 1.34 \cdot 10^{-1}$	s^{-1}	constante de désintégration des précurseurs[a]
γ_4	$= 3.31 \cdot 10^{-1}$	s^{-1}	constante de désintégration des précurseurs[a]
γ_5	$= 1.26$	s^{-1}	constante de désintégration des précurseurs[a]
γ_6	$= 3.21$	s^{-1}	constante de désintégration des précurseurs[a]

[a]Ces paramètres sont communément symbolisés par des lettres grecques lambda à la place des lettres grecques gamma. Ici, des lettres grecques gamma sont utilisées afin d'éviter les confusions avec des taux de défaillance.

Tableau IV.3.5. Conditions initiales au temps $t = t_0$ pour les états stationnaires des variables du processus

variable du processus	expression	valeur initiale	unité
$\omega(t_0)$	$= C_M / K$	$= 6{,}000$	$rad \cdot s^{-1}$
$G(t_0)$	.	$= 4{,}000$	$kg \cdot m^{-2} \cdot s^{-1}$
$T_{c,1}(t_0)$	$= T_e + R \cdot w_1 \cdot P(t_0)$	$= 1{,}437.05$	K
$T_{c,2}(t_0)$	$= T_e + R \cdot w_2 \cdot P(t_0)$	$= 1{,}773.15$	K
$T_1(t_0)$	$= T_e + (w_1 \cdot P(t_0)) / (2 \cdot A_1 \cdot C_R(T_1(t_0)) \cdot G(t_0))$	$= 873$	K
$T_2(t_0)$	$= T_e + (w_2 \cdot P(t_0)) / (2 \cdot A_2 \cdot C_R(T_2(t_0)) \cdot G(t_0))$	$= 873$	K
$P(t_0)$	.	$= 2\,000\,000\,000.00$	W
$C_1(t_0)$	$= (\beta_1 \cdot P(t_0)) / (\Gamma \cdot \gamma_1)$	$= 319\,816\,134.94$	W
$C_2(t_0)$	$= (\beta_2 \cdot P(t_0)) / (\Gamma \cdot \gamma_2)$	$= 1\,203\,444\,877.12$	W
$C_3(t_0)$	$= (\beta_3 \cdot P(t_0)) / (\Gamma \cdot \gamma_3)$	$= 248\,068\,701.72$	W
$C_4(t_0)$	$= (\beta_4 \cdot P(t_0)) / (\Gamma \cdot \gamma_4)$	$= 201\,566\,746.12$	W
$C_5(t_0)$	$= (\beta_5 \cdot P(t_0)) / (\Gamma \cdot \gamma_5)$	$= 24\,519\,422.51$	W
$C_6(t_0)$	$= (\beta_6 \cdot P(t_0)) / (\Gamma \cdot \gamma_6)$	$= 2\,964\,980.67$	W

$$\frac{d}{dt}G(t) = \frac{\upsilon \cdot G(t)^2}{G(t_0)} + C_{nt2} \cdot \left(\omega(t)^2 - \omega(t_0)^2\right) - \upsilon \cdot G(t_0) \qquad \text{[IV.3.17]}$$

La température du combustible dans le canal *i*, notée $T_{c,i}(t)$ [K], avec $i = 1, 2$, est donnée par :

$$\frac{d}{dt}T_{c,i}(t) = \frac{R \cdot w_i \cdot P(t) - \left(T_{c,i}(t) - T_e\right)}{\tau_i\left(T_{c,i}(t)\right)} \qquad \text{[IV.3.18]}$$

La température du sodium dans le canal *i*, notée $T_i(t)$ [K], avec $i = 1, 2$, est donnée par :

$$\frac{d}{dt}T_i(t) = \frac{w_i \cdot P(t)}{2 \cdot A_i \cdot \tau_i\left(T_{c,i}(t)\right) \cdot C_R\left(T_i(t)\right) \cdot G(t)} - \left(\frac{1}{G(t)} \cdot \frac{d}{dt}G(t) + \frac{1}{\tau_i\left(T_{c,i}(t)\right)}\right) \cdot \left(T_i(t) - T_e\right) \qquad \text{[IV.3.19]}$$

La puissance générée par le cœur du réacteur, notée $P(t)$ [W], est donnée par :

$$\frac{d}{dt}P(t) = \left(-\gamma_{SCM} \cdot t \cdot I_1\left(SSCM(t) = 5\right) - \sum_{i=1}^{6}\beta_i\right) \cdot \frac{P(t)}{\Gamma} + \sum_{i=1}^{6}\left[\ \gamma_i \cdot C_i(t)\ \right] \qquad \text{[IV.3.20]}$$

avec *SCM(t)*, la variable d'état du SCRAM, définie dans la Section IV.3.3.1.2 (cf. Tableau IV.3.2).

La concentration du précurseur *i*, notée $C_i(t)$ [W], avec $i = 1, 2, 3, 4, 5, 6$, est donnée par :

$$\frac{d}{dt}C_i(t) = -\gamma_i \cdot C_i(t) + \frac{\beta_i}{\Gamma} \cdot P(t) \qquad \text{[IV.3.21]}$$

À noter que l'introduction d'une fonction indicatrice I_1(A) a permis de n'utiliser qu'un seul jeu d'équations pour la définition des variables du processus, qui dépendent des variables d'état des composants en tant que paramètres. Ces équations dépendent aussi de variables de déviation, et explicitement du temps *t* (pour l'Équation IV.3.20). Plusieurs dérivées de variables du processus sont exprimées en fonction d'autres variables du processus et de leurs dérivées. En effet, il est parfois impossible de fournir une forme explicite de ce type d'équations. Cependant, ces dépendances peuvent être aisément prises en compte en utilisant le formalisme présenté dans la Section IV.3.2.1, lorsque les variables sont modélisées séparément, et avec l'aide des méta-transitions qui rendent disponibles les dérivées en tant que variables supplémentaires.

Enfin, les Équations IV.3.16 à IV.3.21 conviennent à l'étude des scénarios développés dans la suite, mais ne sont pas applicables en l'état pour tous les autres cas. En particulier, ces équations ne sont valables que si les températures du sodium dans les canaux ($T_1(t)$ et $T_2(t)$) sont inférieures à *1 156* K, et les températures du combustible dans les canaux ($T_{c,1}(t)$ et $T_{c,2}(t)$) sont inférieures à *3 070* K.

IV.3.3.1.4. Variables d'information

Treize variables d'information sont utilisées : les résultats de mesure des trois capteurs-transmetteurs ($G^m(t)$, $T_1^m(t)$, et $T_2^m(t)$), les signaux des trois contrôleurs ($y_{CG}(t)$, $y_{CT}(t)$, et $y_{SDL}(t)$), trois données stockées qui correspondent aux résultats de mesure obtenus au précédent instant de temps ($G^d(t)$, $T_1^d(t)$, et $T_2^d(t)$), deux données de traitement qui sont calculées par les capteurs-transmetteurs de température afin de détecter de potentielles dérives ($\alpha_1(t)$ et $\alpha_2(t)$), et deux paramètres de correction utilisés pour compenser les dérives supposées ($T_1^c(t)$ et $T_2^c(t)$). Le vecteur des variables d'information au temps *t* est donc : $\boldsymbol{y(t)} = (G^m(t), T_1^m(t), T_2^m(t), y_{CG}(t), y_{CT}(t), y_{SDL}(t), G^d(t), T_1^d(t), T_2^d(t), \alpha_1(t), \alpha_2(t), T_1^c(t), T_2^c(t))^T$, avec $\boldsymbol{y(t)} \in \mathbb{R}^L$ et $L = 13$. Les variables d'information sont modélisées séparément et définie par les équations qui suivent.

Les résultats de mesure du capteur-transmetteur de flux, notés $G^m(t)$ [kg·m^{-2}·s^{-1}], sont donnés par :

$$G^m(t) = G(t) \cdot I_1(SSG(t) = 1) + {}^{-}G^m(t) \cdot I_1(SSG(t) = 0) + G_{min} \cdot I_1(SSG(t) = 2) \quad [IV.3.22]$$

avec ${}^{-}G^m(t)$, les résultats de mesure ($G^m(t)$) obtenus au précédent instant de temps, c'est-à-dire que ${}^{-}G^m(t) = G^m(t - \varepsilon)$ avec ε qui tend vers 0^+ (cf. Section IV.3.1.1). (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1 : $\varepsilon = \Delta t$ et ${}^{-}G^m(t + \Delta t) = G^m(t)$.) D'après les états des composants donnés dans le Tableau IV.3.2, lorsque le capteur-transmetteur de flux est dans un état *opérant* ($SSG(t) = 1$), il transmet des résultats de mesure corrects, c'est-à-dire que les résultats de mesure sont égaux au flux de sodium ($G^m(t) = G(t)$) ; lorsqu'il est dans un état de *défaillance dangereuse* ($SSG(t) = 0$), il transmet des résultats de mesure qui sont égaux aux précédentes valeurs ($G^m(t) = {}^{-}G^m(t)$) ; et lorsqu'il est dans un état de *défaillance sûre* ($SSG(t) = 2$), il transmet la valeur seuil ($G^m(t) = G_{min}$), ou une valeur qui est en deçà ($G^m(t) < G_{min}$, ce qui implique les mêmes conséquences sur le comportement du système que $G^m(t) = G_{min}$, d'après les équations qui suivent).

Les résultats de mesure du capteur-transmetteur de température i, notés $T_i^m(t)$ [K], avec $i = 1, 2$, sont donnés par :

$$T_i^m(t) = (T_i(t) + T_i^c(t)) \cdot I_1(SSTi(t) = 1, 2, \text{ ou } 4) - \delta_{Di}(t) \cdot I_1(SSTi(t) = 3) + \delta_{Di}(t) \cdot I_1(SSTi(t) = 4) + {}^{-}T_i^m(t) \cdot I_1(SSTi(t) = 0) + T_{max} \cdot I_1(SSTi(t) = 2) \quad [IV.3.23]$$

avec $T_i^c(t)$, les paramètres de correction (variables d'information), définis ci-après ; $\delta_{Di}(t)$, les variables de déviation qui sont les dérives des capteurs-transmetteurs de température, définies dans la Section IV.3.3.1.5 ; et ${}^{-}T_i^m(t)$, les résultats de mesure ($T_i^m(t)$) obtenus au précédent instant de temps, c'est-à-dire ${}^{-}T_i^m(t) = T_i^m(t - \varepsilon)$ avec ε qui tend vers 0^+ (cf. Section IV.3.1.1). (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1 : $\varepsilon = \Delta t$ et ${}^{-}T_i^m(t + \Delta t) = T_i^m(t)$.) D'après les états des composants donnés dans le Tableau IV.3.2, et les « fonctionnalités intelligentes » des capteurs-transmetteurs de température, lorsqu'un capteur-transmetteur de température est dans un état *opérant* ($SSTi(t) = 1$), il transmet des résultats de mesure égaux à la température du sodium dans le canal i, auxquels est ajouté le paramètre de correction des dérives ($T_i^m(t) = T_i(t) + T_i^c(t)$) ; lorsqu'il est dans un état *dégradé* ($SSTi(t) = 3$ ou 4), les résultats sont, de plus, sujets à des dérives négatives ou positives ($T_i^m(t) = T_i(t) + T_i^c(t) - \delta_{Di}(t)$ ou $T_i^m(t) = T_i(t) + T_i^c(t) + \delta_{Di}(t)$) ; lorsqu'il est dans un état de *défaillance dangereuse* ($SSTi(t) = 0$), il transmet des résultats de mesure qui sont égaux aux précédentes valeurs ($T_i^m(t) = {}^{-}T_i^m(t)$) ; et lorsqu'il est dans un état de *défaillance sûre* ($SSTi(t) = 2$), il transmet la valeur seuil ($T_i^m(t) = T_{max}$), ou une valeur qui est au delà ($T_i^m(t) > T_{max}$, ce qui implique les mêmes conséquences sur le comportement du système que $T_i^m(t) = T_{max}$, d'après les équations qui suivent).

Les signaux envoyés par le contrôleur de flux, noté $y_{CG}(t)$, par le contrôleur de température, noté $y_{CT}(t)$, et par l'unité centrale de contrôle, noté $y_{SDL}(t)$, sont donnés par :

$$y_{CG}(t) = I_1(G^m(t) \leq G_{min}) \cdot I_1(SCG(t) = 1) + I_1(SCG(t) = 2) \quad [IV.3.24]$$

$$y_{CT}(t) = I_1((T_1^m(t) \geq T_{max}) \text{ ou } (T_2^m(t) \geq T_{max})) \cdot I_1(SCT(t) = 1) + I_1(SCT(t) = 2) \quad [IV.3.25]$$

$$y_{SDL}(t) = I_1((y_{CG}(t) = 1) \text{ ou } (y_{CT}(t) = 1)) \cdot I_1(SSDL(t) = 1) + I_1(SSDL(t) = 2) \quad [IV.3.26]$$

D'après le Tableau IV.3.2, lorsque le contrôleur de flux (respectivement, le contrôleur de température) est dans un état *opérant* ($SCG(t) = 1$, respectivement $SCT(t) = 1$), il envoie un signal correct, c'est-à-dire qui est égal à 1 si la valeur seuil du flux (respectivement, la valeur seuil de température) est atteinte ou dépassée par les résultats de mesure du capteur-transmetteur correspondant, et égal à 0 sinon ($y_{CG}(t) = I_1(G^m(t) \leq G_{min})$, respectivement $y_{CT}(t) = I_1((T_1^m(t) \geq T_{max})$

ou $(T_2^m(t) \geq T_{max}))$) ; lorsque l'unité centrale de contrôle est dans un état *opérant* ($SSDL(t) = 1$), elle envoie un signal correct, c'est-à-dire qui est égal à *1* si au moins un des contrôleurs primaires (CG et CT) envoie un signal égal à *1*, et *0* sinon ($y_{SDL}(t) = I_1((y_{CG}(t) = 1)$ ou $(y_{CT}(t) = 1))$) ; lorsqu'un contrôleur est dans un état de *défaillance dangereuse* ($SCG(t) = 0$, $SCT(t) = 0$, ou $SSDL(t) = 0$), il envoie un signal qui est égal à *0* (respectivement, $y_{CG}(t) = 0$, $y_{CT}(t) = 0$, et $y_{SDL}(t) = 0$), (d'après la définition de la fonction indicatrice I_1(A), ces cas sont implicitement inclus dans les Équations IV.3.24 à IV.3.26) ; et lorsque le contrôleur est dans un état de *défaillance sûre* ($SCG(t) = 2$, $SCT(t) = 2$, ou $SSDL(t) = 2$), il envoie un signal qui est égal à *1* (respectivement, $y_{CG}(t) = 1$, $y_{CT}(t) = 1$, et $y_{SDL}(t) = 1$).

L'Équation IV.3.23 montre que les résultats de mesure des capteurs-transmetteurs de température peuvent être sujets à des dérives ($\delta_{D1}(t)$ et $\delta_{D2}(t)$) et, pour compenser ces dernières, des paramètres de correction ($T_1^c(t)$ et $T_2^c(t)$) sont ajoutés aux résultats. Ces paramètres de correction des dérives sont calculés en utilisant les « fonctionnalités intelligentes » des capteurs-transmetteurs, selon la procédure suivante :

1. les trois capteurs-transmetteurs (SG, ST1, et ST2) stockent leurs résultats de mesure obtenus aux précédents instants de temps, notés respectivement $G^d(t)$, $T_1^d(t)$, et $T_2^d(t)$;
2. le capteur-transmetteur de flux (SG) transmet ses résultats de mesure courants et précédents ($G^m(t)$ et $G^d(t)$) aux deux capteurs-transmetteurs de température ;
3. chaque capteur-transmetteur de température *i* (STi), avec $i = 1, 2$, calcule des données de traitement, notées $\alpha_i(t)$, d'après leurs résultats de mesure courants et précédents ($T_i^m(t)$ et $T_i^d(t)$), et les données reçues du capteur-transmetteur de flux ($G^m(t)$ et $G^d(t)$), afin de détecter de potentielles dérives dans les résultats de mesure ;
4. les capteurs-transmetteurs de température (ST1 et ST2) se transmettent mutuellement leurs données de traitement ($\alpha_1(t)$ et $\alpha_2(t)$), et leurs résultats de mesure courants ($T_1^m(t)$ et $T_2^m(t)$) ;
5. chaque capteur-transmetteur de température *i* (STi), avec $i = 1, 2$, calcule un paramètre de correction, noté $T_i^c(t)$, d'après l'ensemble des données de traitement ($\alpha_1(t)$ et $\alpha_2(t)$), et des résultats de mesure courants ($T_1^m(t)$ et $T_2^m(t)$), afin de compenser les dérives supposées dans ses résultats de mesure.

Les données stockées correspondent donc aux résultats de mesure obtenus au précédent instant de temps, pour le capteur-transmetteur de flux, notées $G^d(t)$ [kg·m^{-2}·s^{-1}], et pour le capteur-transmetteur de température *i*, notées $T_i^d(t)$ [K], avec $i = 1, 2$, c'est-à-dire que :

$$G^d(t) = {}^{-}G^m(t) \qquad \text{[IV.3.27]}$$

$$T_i^d(t) = {}^{-}T_i^m(t) \qquad \text{[IV.3.28]}$$

À noter qu'il est aussi possible de définir $G^d(t)$ et $T_i^d(t)$ en utilisant des valeurs plus anciennes de $G^m(t)$ et de $T_i^m(t)$, en utilisant des conditions sur le temps *t*, ce qui peut être aisément pris en compte en utilisant le formalisme présenté dans la Section IV.3.2.1.

Les données de traitement $\alpha_i(t)$, avec $i = 1, 2$, évaluent les dérivées des résultats de mesure du capteur-transmetteur de température *i*, d'après $T_i^m(t)$ et $T_i^d(t)$, et les comparent avec les dérivées théoriques obtenues par l'Équation IV.3.19, en utilisant $T_i^m(t)$, $T_i^d(t)$, $G^m(t)$, et $G^d(t)$, à la place des valeurs « vraies » (et inconnues) des variables du processus. Pour cela, les paramètres du Tableau IV.3.4 sont supposés connus, tout comme les conditions initiales données dans le Tableau IV.3.5. De plus, d'après les Équations IV.3.18, IV.3.20, et IV.3.21, et le Tableau IV.5, il est montré que les variables du processus $T_{c,i}(t)$, avec $i = 1, 2$, et $P(t)$, sont constantes et respectivement égales à $T_{c,i}(t_0)$ et $P(t_0)$, (indépendamment des variables de déviation), jusqu'à l'activation de SCRAM (la période

de temps après l'activation du SCRAM n'est plus concernée par la fonction de sécurité). Tous les paramètres sont donc disponibles pour calculer $\alpha_i(t)$, avec $i = 1, 2$:

$$\alpha_i(t) = \frac{T_i^m(t) - T_i^d(t)}{\varepsilon} - B_i(t) \qquad \text{[IV.3.29]}$$

avec :

$$B_i(t) = \frac{w_i \cdot P(t_0)}{2 \cdot A_i \cdot \tau_i\left(T_{c,i}(t_0)\right) \cdot C_R\left(T_i^m(t)\right) \cdot G^m(t)} - \left(\frac{G^m(t) - G^d(t)}{G^m(t) \cdot \varepsilon} + \frac{1}{\tau_i\left(T_{c,i}(t_0)\right)} \right) \cdot \left(T_i^m(t) - T_e\right) \qquad \text{[IV.3.30]}$$

avec ε qui tend vers 0^+. (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1, et d'après les Équations IV.3.27 et IV.3.28 : $\varepsilon = \Delta t$.) Des analyses ont alors montré que des caractéristiques sur les résultats de mesure $T_1^m(t)$, $T_2^m(t)$, et $G^m(t)$, pouvaient être déduites des données de traitement $\alpha_1(t)$ et $\alpha_2(t)$, telles que données dans le Tableau IV.3.6.

D'après l'Équation IV.3.19 et le Tableau IV.3.5, les températures $T_1(t)$ et $T_2(t)$ sont quasi égales (indépendamment des variables de déviation) jusqu'à l'activation du SCRAM (cf. résultats empiriques présentés dans la Section IV.3.3.2.3). Il est alors proposé d'utiliser les données de traitement ($\alpha_1(t)$ et $\alpha_2(t)$) afin de détecter de potentielles dérives dans les résultats de mesure ($T_1^m(t)$ et $T_2^m(t)$) et, le cas échéant, de définir des paramètres de correction des dérives ($T_1^c(t)$ et $T_2^c(t)$), de telle sorte que les résultats de mesure soient égaux entre eux. D'après le Tableau IV.3.6, différentes hypothèses peuvent être faites sur les dérives des résultats de mesure, en fonction des données de traitement ($\alpha_1(t)$ et $\alpha_2(t)$). Ces hypothèses sont alors utilisées pour définir les paramètres de correction des dérives ($T_1^c(t)$ et $T_2^c(t)$), d'après les règles données dans le Tableau IV.3.7. Si des dérives sont (exclusivement) supposées dans les résultats de mesure du capteur-transmetteur de température *1* (respectivement, pour le capteur-transmetteur de température *2*), alors le paramètre de correction des dérives $T_1^c(t)$ (respectivement, $T_2^c(t)$) est modifié de telle sorte que $T_1^m(t)$ devienne égal à $T_2^m(t)$, c'est-à-dire que $T_1^c(t) = T_2^m(t) - T_1^m(t)$, (respectivement, $T_2^c(t) = T_1^m(t) - T_2^m(t)$). Si des dérives sont supposées dans les résultats de mesure des deux capteurs-transmetteurs de température, alors les paramètres de correction des dérives $T_1^c(t)$ et $T_2^c(t)$ sont modifiés tous les deux de telle sorte que $T_1^m(t)$ et $T_2^m(t)$ deviennent égales à $(T_1^m(t) + T_2^m(t)) / 2$, c'est-à-dire que $T_1^c(t) = (T_2^m(t) - T_1^m(t)) / 2$ et $T_2^c(t) = (T_2^m(t) - T_2^m(t)) / 2$. Dans les autres cas, les paramètres de correction des dérives restent inchangés ($T_1^c(t) = {}^{-}T_1^c(t)$ et $T_2^c(t) = {}^{-}T_2^c(t)$).

Un parallèle peut être observé entre les variables d'information définies dans cette section, et le modèle générique pour les CTI présenté dans la Section IV.3.2.2 (cf. Figure IV.3.4). Par exemple, en considérant la modélisation du capteur-transmetteur de température *i* (STi), avec $i = 1, 2$, les résultats de mesure $T_i^m(t)$ correspondent au sous-ensemble *(M)* des variables d'information ; les données stockées $T_i^d(t)$ au sous-ensemble *(D)* ; les données de traitement $\alpha_i(t)$ au sous-ensemble *(P)* ; les paramètres de correction $T_i^c(t)$ au sous-ensemble *(C)* ; et les informations transmises aux autres éléments du systèmes (aux autres capteurs-transmetteurs) sont constituées de $T_i^c(t)$ et de $\alpha_i(t)$, et correspondent au sous-ensemble *(I)*. Le paramètre α_{ref} (utilisé comme critère pour la définition des paramètres de correction des dérives $T_i^c(t)$, cf. Tableau IV.3.7) peut être considéré soit comme un paramètre fixé, c'est-à-dire qui n'est pas représenté par une variable dans le modèle, soit comme une variable d'entrée (par exemple, qui peut être modifiée par un utilisateur), c'est-à-dire qui est représenté par une variable d'information reçue par d'autres éléments du système (sous-ensemble $\backslash(T)$ du vecteur $\boldsymbol{y(t)}$). Dans de futurs développements, d'autres variables d'information pourraient être considérées, par exemple pour détecter un état de *défaillance* du capteur-transmetteur lorsque le paramètre de correction des dérives $T_i^c(t)$ dépasse un certain seuil. De même, aucun paramètre de reconfiguration (sous-ensemble *(R)*) n'est utilisé dans le présent cas d'étude. De tels paramètres

Tableau IV.3.6. Relations entre les données de traitement $\alpha_i(t)$ et les résultats de mesure $T_i^m(t)$ et $G^m(t)$, avec $i = 1, 2$

résultats de mesure[a] $T_i^m(t)$ et $G^m(t)$	donnée de traitement $\alpha_i(t)$
$T_i^m(t) = T_i(t)$ et $G^m(t) = G(t)$	$\alpha_i(t) = 0$
$T_i^m(t) < T_i(t)$ ou $G^m(t) > G(t)$	$\alpha_i(t) < 0$
$T_i^m(t) > T_i(t)$ ou $G^m(t) < G(t)$	$\alpha_i(t) > 0$

[a]D'autres combinaisons d'évènements du second degré telles que $\{T_i^m(t) < T_i(t)$ et $G^m(t) < G(t)\}$ ou $\{T_i^m(t) > T_i(t)$ et $G^m(t) > G(t)\}$ conduisent à des effets indéterminés sur les données de traitement $\alpha_i(t)$, car dépendent des écarts entre $T_i^m(t)$ et $T_i(t)$, et entre $G^m(t)$ et $G(t)$.

Tableau IV.3.7. Définition des paramètres de correction des dérives $T_i^c(t)$ [K], d'après les données de traitement $\alpha_i(t)$, avec $i = 1, 2$

critères[a] sur les données de traitement $\alpha_i(t)$	hypothèses acceptées[b]	paramètres de correction $T_i^c(t)$
$\alpha_1(t) < -\alpha_{ref}$ et $\alpha_2(t) < -\alpha_{ref}$	$G^m(t) > G(t)$	$T_i^c(t) = {}^{-}T_i^c(t)$ pour $i = 1, 2$
$\alpha_1(t) > \alpha_{ref}$ et $\alpha_2(t) > \alpha_{ref}$	$G^m(t) < G(t)$	$T_i^c(t) = {}^{-}T_i^c(t)$ pour $i = 1, 2$
$\lvert\alpha_1(t)\rvert > \alpha_{ref}$ et $\lvert\alpha_2(t)\rvert < \alpha_{ref}$	$T_1^m(t) < T_1(t)$ ou $T_1^m(t) > T_1(t)$	$T_1^c(t) = T_2^m(t) - T_1^m(t)$ et $T_2^c(t) = {}^{-}T_2^c(t)$
$\lvert\alpha_1(t)\rvert < \alpha_{ref}$ et $\lvert\alpha_2(t)\rvert > \alpha_{ref}$	$T_2^m(t) < T_2(t)$ ou $T_2^m(t) > T_2(t)$	$T_1^c(t) = {}^{-}T_1^c(t)$ et $T_2^c(t) = T_1^m(t) - T_2^m(t)$
$\alpha_1(t) < -\alpha_{ref}$ et $\alpha_2(t) > \alpha_{ref}$	$T_1^m(t) < T_1(t)$ et $T_2^m(t) > T_2(t)$	$T_1^c(t) = (T_2^m(t) - T_1^m(t)) / 2$ et $T_2^c(t) = (T_1^m(t) - T_2^m(t)) / 2$
$\alpha_1(t) > \alpha_{ref}$ et $\alpha_2(t) < -\alpha_{ref}$	$T_1^m(t) > T_1(t)$ et $T_2^m(t) < T_2(t)$	$T_1^c(t) = (T_2^m(t) - T_1^m(t)) / 2$ et $T_2^c(t) = (T_1^m(t) - T_2^m(t)) / 2$
autres cas	$T_1^m(t) = T_1(t)$ et $T_2^m(t) = T_2(t)$	$T_i^c(t) = {}^{-}T_i^c(t)$ pour $i = 1, 2$

[a]Avec le paramètre α_{ref} introduit dans la Section IV.3.3.1.4.
[b]L'acceptation de ces hypothèses est définit à partir du Tableau IV.3.6, basé sur une équiprobabilité a priori des évènements suivants : $\{G^m(t) < G(t)\}$, $\{G^m(t) > G(t)\}$, $\{T_i^m(t) < T_i(t)\}$, et $\{T_i^m(t) > T_i(t)\}$, pour $i = 1, 2$.

pourraient, par exemple, servir à commander une redondance passive du capteur-transmetteur si ce dernier est détecté dans un état de *défaillance*.

IV.3.3.1.5. Variables de déviation

Trois variables de déviation sont utilisées : les déviations du couple de la pompe ($\delta_M(t)$, cf. Équation IV.3.16), et les dérives des capteurs-transmetteurs de température ($\delta_{D1}(t)$ et $\delta_{D2}(t)$, cf. Équation IV.3.23). Les vecteur des variables de déviation au temps t est donc $\boldsymbol{e(t)} = (\delta_M(t), \delta_{D1}(t), \delta_{D2}(t))^T$, avec $\boldsymbol{e(t)} \in \mathbb{R}^Q$ et $Q = 3$. Les variables de déviation sont modélisées séparément, et définies par des processus stochastiques.

Les déviations du couple de la pompe, notées $\delta_M(t)$ [N·m], sont données par :

$$\delta_M(t + dt) = \delta_M(t) + E_M(\alpha_M \cdot dt, \beta_M) \cdot I_1(\delta_M(t) < C_M) \cdot I_1(SPM(t) = 3) \quad \text{[IV.3.31]}$$

avec $SPM(t)$, la variable d'état de la pompe, définie dans la Section IV.3.3.1.2 (cf. Tableau IV.3.2) ; $E_M(\alpha_M \cdot dt, \beta_M)$, une variable aléatoire distribuée selon une loi Gamma de paramètre de forme $\alpha_M \cdot dt = 0.5 \cdot dt$ et de paramètre d'échelle $1/\beta_M = 400.0$ [N.m] ; et C_M, le couple nominale de la pompe, donné dans le Tableau IV.3.4. D'après l'Équation IV.3.16, le couple total de la pompe est donc égal à $C_M - \delta_M(t)$ lorsque $SPM(t) = 3$. Comme l'incrément des déviations du couple de la pompe dans l'intervalle de temps $[t ; t + dt]$, défini par $E_M(\alpha_M \cdot dt, \beta_M) \cdot I_1(\delta_M(t) < C_M) \cdot I_1(SPM(t) = 3)$, est indépendant du temps t (mais, évidement, fonction de dt), ce processus stochastique est stationnaire, étant donné $I_1(\delta_M(t) < C_M) \cdot I_1(SPM(t) = 3)$. (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1 : $dt = \Delta t$.)

Les dérives du capteur-transmetteur de température i, notées $\delta_{Di}(t)$ [K], avec $i = 1, 2$, sont données par :

$$\delta_{Di}(t + dt) = \delta_{Di}(t) + E_D(\alpha_D \cdot dt, \beta_D(\delta_{Di}(t), T_i(t))) \cdot I_1(SSTi(t) = 3 \text{ ou } 4) \quad \text{[IV.3.32]}$$

avec $SSTi(t)$, la variable d'état du capteur-transmetteur de température i, définie dans la Section IV.3.3.1.2 (cf. Tableau IV.3.2) ; $T_i(t)$, la variable du processus qui est la température du sodium dans le canal i, définie dans la Section IV.3.3.1.3 ; et $E_D(\alpha_D \cdot dt, \beta_D(\delta_{Di}(t), T_i(t)))$, une variable aléatoire distribuée selon une loi Gamma de paramètre de forme $\alpha_D \cdot dt = 1.0 \cdot dt$ et de paramètre d'échelle $1/\beta_D(\delta_{Di}(t), T_i(t)) = (T_i(t) \cdot (\delta_{Di}(t) + 20.0)) / 3.0 \cdot 10^4$ [K], avec $i = 1, 2$. (Pour les analyses numériques en utilisant le formalisme présenté dans la Section IV.3.2.1 : $dt = \Delta t$.)

IV.3.3.2. Modélisation et analyses appliquées au cas d'étude

IV.3.3.2.1. Modélisation de la fiabilité dynamique

Le système a été modélisé en utilisant le formalisme présenté dans la Section IV.3.2.1, et le réseau de Petri correspondant décrit sur la Figure IV.3.6. En accord avec ce formalisme, chaque variable a été modélisée séparément (excepté pour les concentrations des précurseurs $C_i(t)$, avec $i = 1, 2, 3, 4, 5, 6$, qui ont été modélisées par un vecteur, noté $\boldsymbol{C(t)}$). Les variables du processus sont décrites sur la partie gauche de la Figure IV.3.6, et peuvent être distinguées par des places grises, de traits continus, et qui sont associées à des méta-transitions (cf. légende de la Figure IV.3.1). La méta-transition associée à la variable du flux de sodium ($G(t)$) a été explicitement représentée parce que la dérivée incluse dans cette méta-transition ($G'(t)$) est utilisée pour calculer les évolutions des températures du sodium ($T_1(t)$ et $T_2(t)$). Les variables de déviation peuvent être distinguées par des places blanches et des traits continus ; les variables d'état des composants par des places blanches et

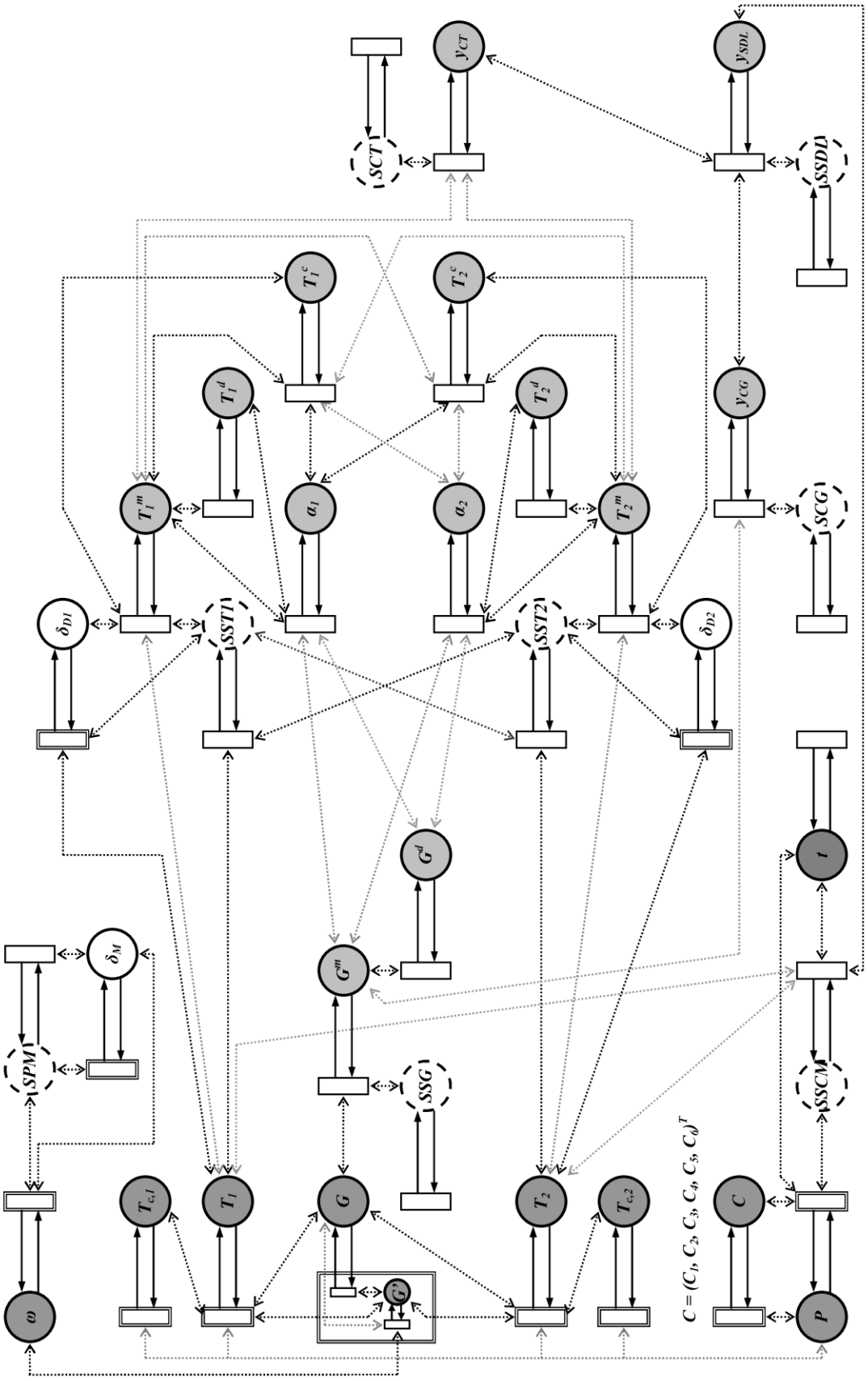

Figure IV.3.6. Réseau de Petri pour la modélisation de la fiabilité dynamique du cas d'étude

des traits discontinus ; et les variables d'information par des places gris clair, de traits continus, et qui sont associées à des transitions qui ne sont pas des méta-transitions (cf. Figure IV.3.1). Enfin, la variable du temps *t* a été également représentée, et affecte directement la variable d'état du SCRAM (*SSCM(t)*, cf. Tableau IV.3.3) et la puissance générée par le cœur du réacteur (*P(t)*, cf. Équation IV.3.20).

Dans un souci de lisibilité, la spécification des gardes des transitions ne sont pas précisées sur la Figure IV.3.6. Cependant, il est considéré que chaque transition est franchie à chaque incrément de temps Δt, et a donc une garde notée $s_i[\Delta t]$, avec des instants de temps s_i qui respectent l'ordre défini dans la Section IV.3.2.1 : les évolutions des variables du processus et de déviation sont calculées en premier ; ensuite les variables d'état des composants ; la variable du temps *t* ; les variables du processus et de déviation ; et enfin, les variables d'information. De plus, parmi les variables de même type, la dérivée du flux de sodium ($G'(t)$) doit être calculée avant les dérivées des températures du sodium ($T_1(t)$ et $T_2(t)$), parce que ces dernières dépendent des premières ; et les variables d'information peuvent, par exemple, être calculées suivant cet ordre : $G^d(t)$, $T_1^d(t)$, $T_2^d(t)$, $G^m(t)$, $T_1^m(t)$, $T_2^m(t)$, (parce que les résultats de mesure doivent être stockés, en accord avec les Équations IV.3.27 et IV.3.28, avant le calcul des nouveaux résultats de mesure, en accord avec les Équations IV.3.22 et IV.3.23), $\alpha_1(t)$, $\alpha_2(t)$, $T_1^c(t)$, $T_2^c(t)$, $y_{CG}(t)$, $y_{CT}(t)$, et $y_{SDL}(t)$. À noter que les paramètres de correction des dérives calculés au temps *t* ($T_1^c(t)$ et $T_2^c(t)$) sont alors appliqués aux résultats de mesure du temps $t + \Delta t$.

La spécification des arcs de sortie ne sont pas plus précisées. D'après les Sections IV.3.1.2 et IV.3.2.1, l'arc de sortie correspondant à chaque variable du processus $\boldsymbol{x(t)}_k$ ($k^{\text{ème}}$ composante du vecteur $\boldsymbol{x(t)}$) doit être spécifié par le membre de droite de l'équation $\boldsymbol{x}(t + \Delta t)_k \approx \boldsymbol{x(t)}_k + \Delta t \cdot \boldsymbol{x'(t)}_k$, avec la dérivée $\boldsymbol{x'(t)}_k$ donnée par l'équation correspondante parmi les Équations IV.3.16 à IV.3.21. De même, l'arc de sortie correspondant à chaque variable de déviation $\boldsymbol{e(t)}_k$ doit être spécifié par le membre de droite de l'équation $\boldsymbol{e}(t + \Delta t)_k = \boldsymbol{e(t)}_k + d\boldsymbol{E(t)}_k$, avec l'incrément aléatoire $d\boldsymbol{E(t)}_k$ donné par l'équation correspondante parmi les Équations IV.3.31 et IV.3.32.

L'arc de sortie utilisé pour modifier la valeur de chaque variable d'état des composants $\boldsymbol{i(t)}_k$ doit être spécifié par le membre de droite de l'équation $\boldsymbol{i}(t + \Delta t)_k = \boldsymbol{P}_{[i_k],i(t)}(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)^T \cdot [\boldsymbol{i}_k]$, avec $[\boldsymbol{i}_k]$ défini par toutes les valeurs possibles de la variable $\boldsymbol{i(t)}_k$, telles que données dans le Tableau IV.3.2, et $\boldsymbol{P}_{[i_k],i(t)}(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)^T$ le vecteur aléatoire défini par la procédure présentée dans la Section IV.3.1.2, en utilisant les taux de transition donnés dans le Tableau IV.3.3. Par exemple, la variable d'état du capteur-transmetteur de flux (*SSG(t)*), (pour cet exemple, $k = 2$ et $\boldsymbol{i(t)}_k = SSG(t)$, d'après la Section IV.3.3.1.2), a $E_{SSG} = 3$ états possibles, et $[SSG] = (1, 0, 2)^T$, d'après le Tableau IV.3.2. Le vecteur aléatoire $\boldsymbol{P}_{[SSG],SSG(t)}$, (pour cet exemple, les variables $\boldsymbol{x(t)}$, $\boldsymbol{y(t)}$, $\boldsymbol{e(t)}$, et *t*, ne sont pas concernées, et seule la composante de $\boldsymbol{i(t)}$ qui correspond à *SSG(t)* est utilisée), est défini selon les valeurs de *SSG(t)*, le Tableau IV.3.3, et la procédure présentée dans la Section IV.3.3.1.2 : si $SSG(t) = 1$ alors $\boldsymbol{\rho}_{[SSG],SSG(t)} = ((1 - \Delta t \cdot (\lambda_{SG,0} + \lambda_{SG,2})), \Delta t \cdot \lambda_{SG,0}, \Delta t \cdot \lambda_{SG,2})^T$, si $SSG(t) = 0$ alors $\boldsymbol{\rho}_{[SSG],SSG(t)} = (0, 1,0)^T$, et si $SSG(t) = 2$ alors $\boldsymbol{\rho}_{[SSG],SSG(t)} = (0, 0,1)^T$; ensuite $R_{[SSG],SSG(t)}$ est une variable aléatoire discrète, d'espace des réalisations $(1, 2, 3)$, et de fonction de masse définie par $\boldsymbol{\rho}_{[SSG],SSG(t)}$; et enfin, $\boldsymbol{P}_{[SSG],SSG(t)}$ est un vecteur dont toutes ses composantes sont égales à *0*, exceptée pour la composante indicée par la réalisation de $R_{[SSG],SSG(t)}$, qui est égale à *1*.

L'arc de sortie correspondant à chaque variable d'information $\boldsymbol{y(t)}_k$ doit être spécifié par le membre de droite de l'équation correspondante parmi les Équations IV.3.22 à IV.3.30, et le Tableau IV.3.7 pour les paramètres de correction des dérives ($T_1^c(t)$ et $T_2^c(t)$), avec $\varepsilon = \Delta t$, $^{-}G^m(t + \Delta t) = G^m(t)$, $^{-}T_1^m(t + \Delta t) = T_1^m(t)$, et $^{-}T_2^m(t + \Delta t) = T_2^m(t)$, d'après le formalisme présenté dans la Section

IV.3.2.1. Enfin, pour l'arc de sortie correspondant à la variable du temps *t*, la spécification est simplement $t + \Delta t$.

En suivant le modèle décrit sur la Figure IV.3.6, le système a été modélisé, et ses évolutions simulées, en utilisant le logiciel CPN Tools [CPN10, KJe07] (cf. Section IV.2.2.1). Celui-ci possède certaines caractéristiques qui ont guidé ce choix :

- capacités de représenter des propriétés colorées ;
- définition explicite de variables et de fonctions (notamment pour la spécification des arcs de sortie), avec la possibilité d'y inclure des propriétés stochastiques ;
- possibilités de créer des réseaux de Petri « hiérarchiques » en attribuant à une transition un réseau de Petri séparé (utile pour représenter des méta-transitions), ou en fusionnant des places (ce qui permet d'améliorer la clarté du modèle) ;
- support à des analyses par simulations de Monte Carlo ;
- capacités d'éditer et de définir des fonctions d'observation et de contrôle (par exemple, pour observer les évolutions de n'importe quelles variables du système) ;
- interface utilisateur relativement ergonomique, qui inclut un éditeur graphique, des vérifications automatiques de syntaxe, et des messages d'erreurs contextuels ;
- logiciel gratuit.

En contrepartie, certains aspects pausent quelques difficultés :

- les modèles construis via CPN Tools ne sont pas capables de prendre en compte des nombres réels et ceux-ci doivent donc être « codés » en utilisant des nombres entiers ;
- les simulations nécessitent souvent un temps important.

Plusieurs analyses du système ont alors été effectuées, et sont présentées dans les sections suivantes. Pour l'ensemble de ces analyses, un incrément de temps de *1* seconde ($\Delta t = 1$ seconde) a été utilisé.

IV.3.3.2.2. Exemples d'évolutions des variables de déviation

Des exemples d'évolutions aléatoires du couple de la pompe ($C_M - \delta_M(t)$) sont décrits sur la Figure IV.3.7, d'après les déviations du couple de la pompe ($\delta_M(t)$) définies par l'Équation IV.3.31, en commençant au temps $t = 0$ avec la pompe dans un état *dégradé*, puis qui reste dans ce même état ($SPM(t) = 3$ pour $t \geq 0$).

Des exemples d'évolutions aléatoires des dérives des capteurs-transmetteurs de température ($\delta_{Di}(t)$) sont décrits sur la Figure IV.3.8, d'après l'Équation IV.3.32, en commençant au temps $t = 0$ avec le capteur-transmetteur de température dans un état de *dérives*, puis qui reste dans ce même état ($SSTi(t) = 3$ ou 4 pour $t \geq 0$), et avec la température du sodium ($T_i(t)$) qui augmente de façon linéaire entre $T_i(0$ seconde$) = 875$ K et $T_i(60$ secondes$) = 935$ K.

IV.3.3.2.3. Exemples de scénarios

Au temps $t = t_0 = 0$ seconde, les composants du système sont dans des états *opérants* (toutes les variables d'état des composants sont égales à *1*), sauf mention contraire dans la suite ; les variables du processus sont dans les conditions initiales données dans le Tableau IV.3.5 ; les variables d'information pour les résultats de mesure et les signaux sont définies par les Équations IV.3.22 à IV.3.26, et les autres variables d'information sont égales à *0.0* ; et les variables de déviation sont égales à *0.0*. Les scénarios suivants ont été simulés pour des évolutions fixées des variables d'états des composants, et les évolutions (simulées) correspondantes du flux de sodium ($G(t)$) et des températures du sodium ($T_1(t)$ et $T_2(t)$) sont décrites sur les Figures IV.3.9 à IV.3.12 :

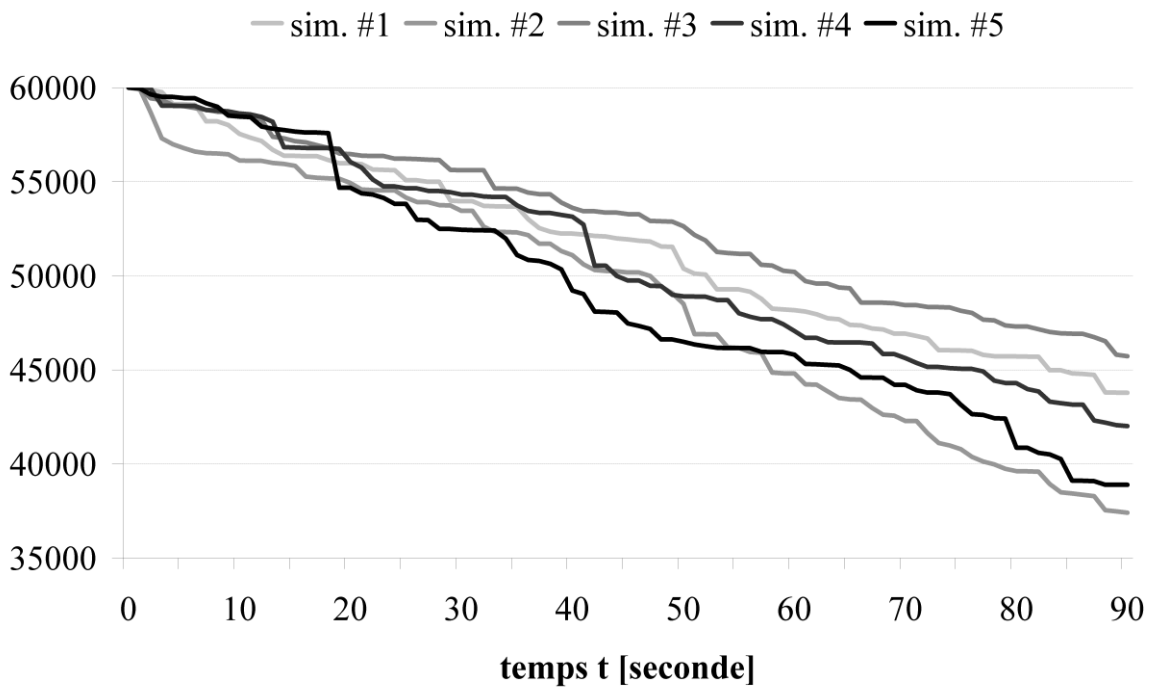

Figure IV.3.7. Exemples de simulations du couple de la pompe ($C_M - \delta_M(t)$) [N·m], lorsque la pompe est dans un état *dégradé*

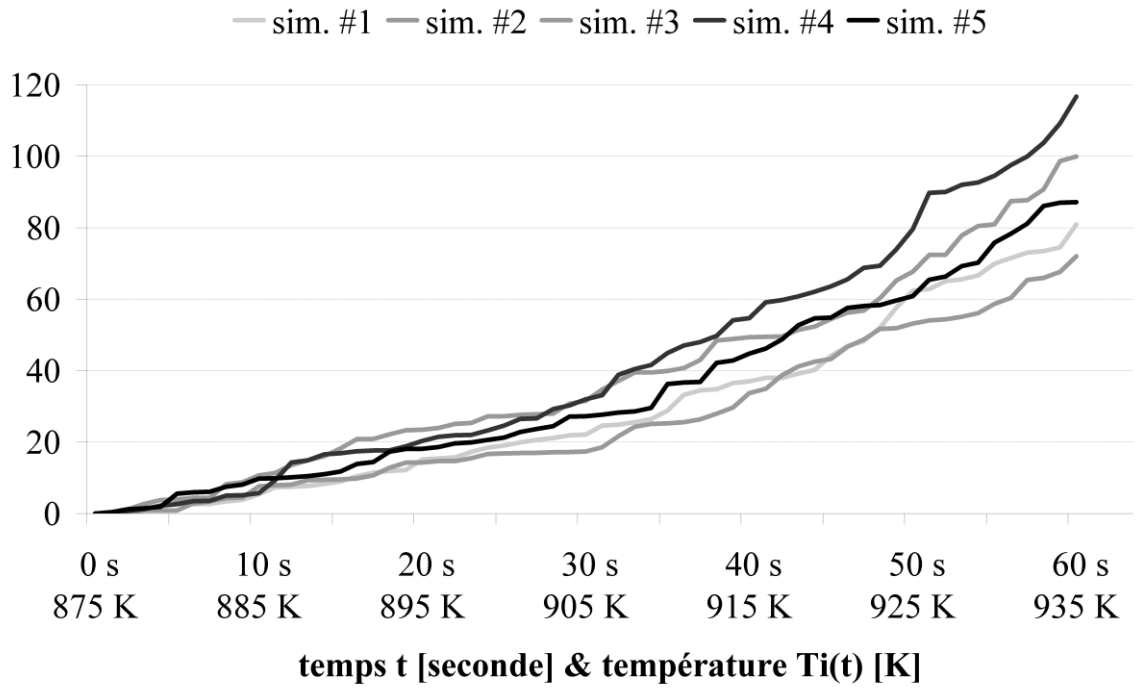

Figure IV.3.8. Exemples de simulations des dérives d'un capteur-transmetteur de température ($\delta_{Di}(t)$) [K], lorsque le capteur-transmetteur est dans un état de *dérives*

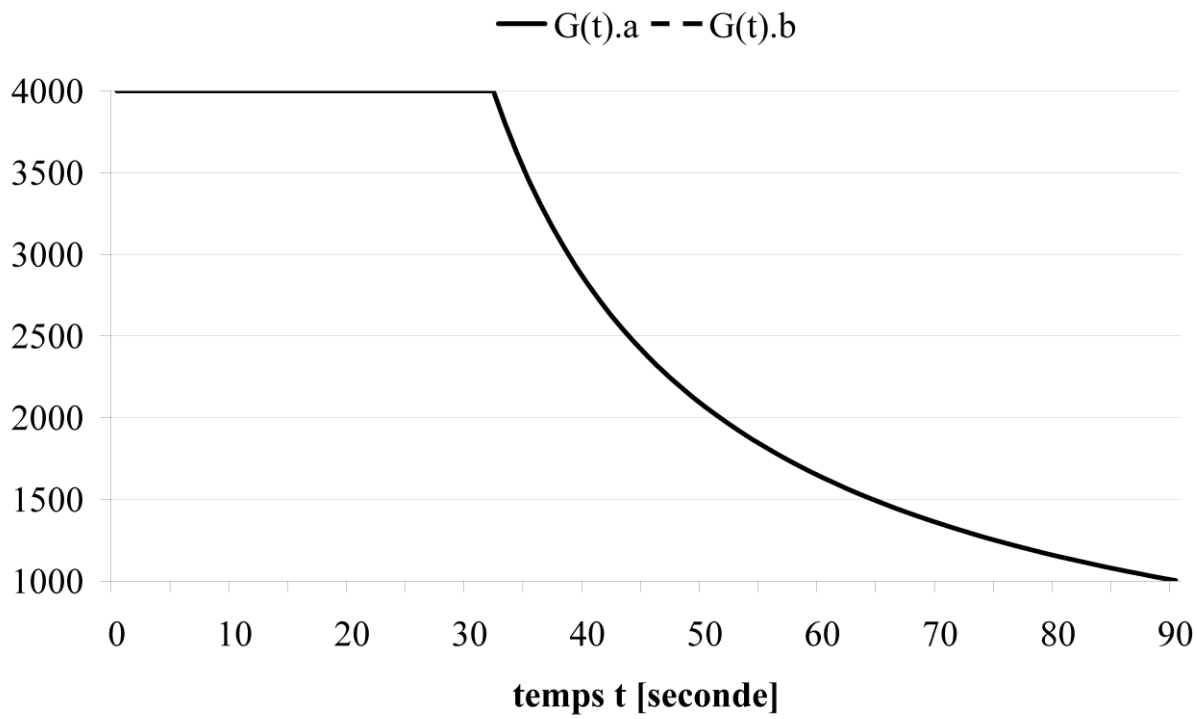

Figure IV.3.9. Évolutions du flux de sodium (*G(t)*) [kg·m^{-2}·s^{-1}] dans les scénarios a et b

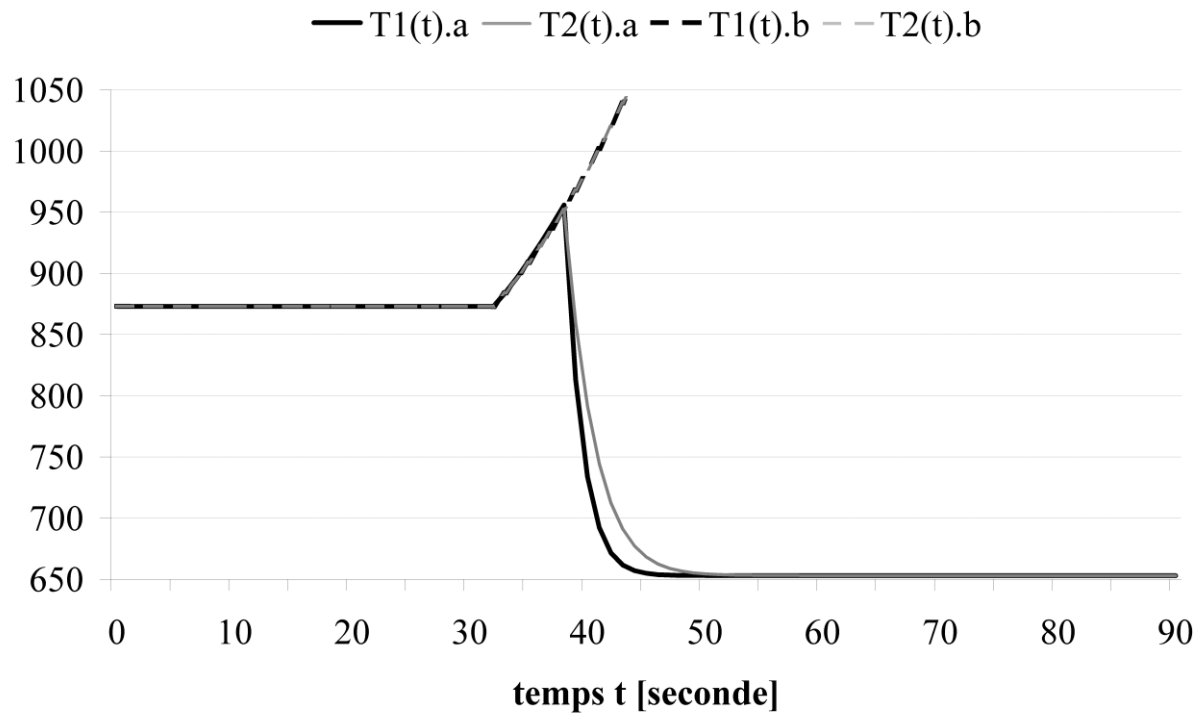

Figure IV.3.10. Évolutions des températures du sodium ($T_1(t)$ et $T_2(t)$) [K] dans les scénarios a et b

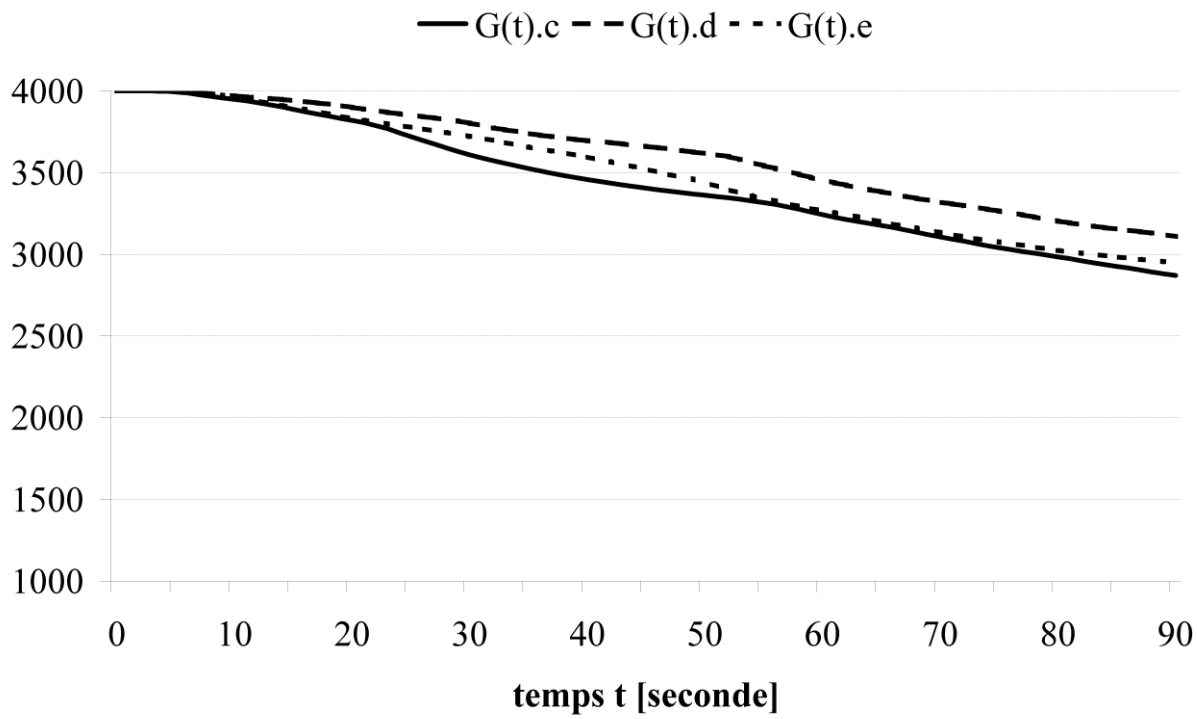

Figure IV.3.11. Évolutions du flux de sodium (*G(t)*) [kg·m^{-2}·s^{-1}] dans les scénarios c, d, et e

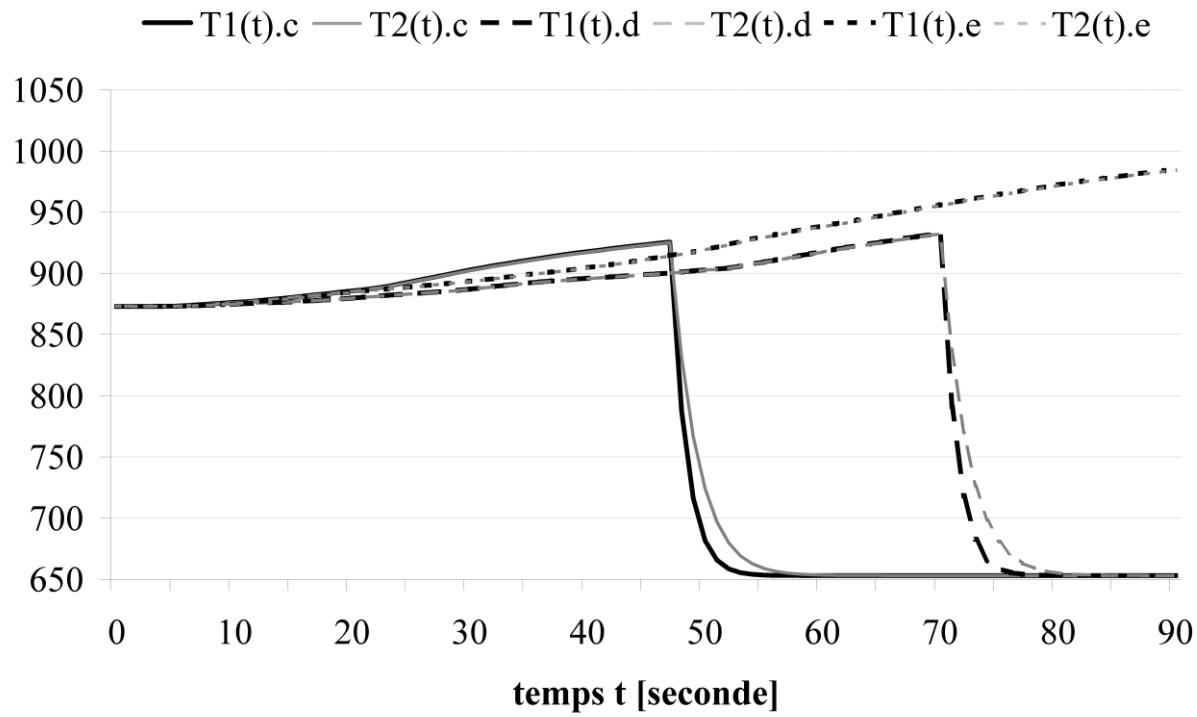

Figure IV.3.12. Évolutions des températures du sodium ($T_1(t)$ et $T_2(t)$) [K] dans les scénarios c, d, et e

a. la pompe reste dans un état *opérant* jusqu'au temps $t = 30$ secondes ($SPM(t) = 1$ pour $t_0 \leq t < 30$ secondes) où une *défaillance totale* de la pompe se produit ($SPM(t) = 0$ pour $t \geq 30$ secondes) ; et le SCRAM est activé au temps $t = 36$ secondes ($SSCM(t) = 1$ pour $t_0 \leq t < 36$ secondes et $SSCM(t) = 5$ pour $t \geq 36$ secondes) avec les variables du processus correspondantes (obtenues par simulations) : $T_1(36 \text{ secondes}) = 924.5$ K, $T_2(36 \text{ secondes}) = 922.5$ K, et $G(36 \text{ secondes}) = 3\,305.9$ kg·m^{-2}·s^{-1} ;
b. la pompe reste dans un état *opérant* jusqu'au temps $t = 30$ secondes ($SPM(t) = 1$ pour $t_0 \leq t < 30$ secondes) où une *défaillance totale* de la pompe se produit ($SPM(t) = 0$ pour $t \geq 30$ secondes) ; et le SCRAM n'est jamais activé ($SSCM(t) \neq 5$ pour $t \geq t_0$) ;
c. la pompe est dans un état *dégradé* au temps t_0 et reste dans cet état ($SPM(t) = 3$ pour $t \geq t_0$) ; et le SCRAM est activé au temps $t = 45$ secondes ($SSCM(t) = 1$ pour $t_0 \leq t < 45$ secondes et $SSCM(t) = 5$ pour $t \geq 45$ secondes) avec les variables du processus correspondantes (obtenues par simulations) : $T_1(45 \text{ secondes}) = 923.5$ K, $T_2(45 \text{ secondes}) = 923.1$ K, et $G(45 \text{ secondes}) = 3\,404.4$ kg·m^{-2}·s^{-1} ;
d. la pompe est dans un état *dégradé* au temps t_0 et reste dans cet état ($SPM(t) = 3$ pour $t \geq t_0$) ; et le SCRAM est activé au temps $t = 68$ secondes ($SSCM(t) = 1$ pour $t_0 \leq t < 68$ secondes et $SSCM(t) = 5$ pour $t \geq 68$ secondes) avec les variables du processus correspondantes (obtenues par simulations) : $T_1(68 \text{ secondes}) = 930.1$ K, $T_2(68 \text{ secondes}) = 929.6$ K, et $G(68 \text{ secondes}) = 3\,342.6$ kg·m^{-2}·s^{-1} ;
e. la pompe est dans un état *dégradé* au temps t_0 et reste dans cet état ($SPM(t) = 3$ pour $t \geq t_0$) ; et le SCRAM n'est jamais activé ($SSCM(t) \neq 5$ pour $t \geq t_0$) ;

Les évolutions du flux de sodium ($G(t)$) dans les scénarios a et b sont respectivement notées $G(t).a$ et $G(t).b$, et sont décrites sur la Figure IV.3.9. D'après les conditions d'états stationnaires, le flux est constant jusqu'à l'occurrence de la *défaillance totale* de la pompe au temps $t = 30$ secondes, puis il décroît en fonction des Équations IV.3.16 et IV.3.17. À noter que d'après ces équations, l'activation du SCRAM n'a pas d'effet sur le flux de sodium, donc $G(t).a = G(t).b$.

Les évolutions des températures du sodium ($T_1(t)$ et $T_2(t)$) dans les scénarios a et b sont respectivement notées $T_1(t).a$, $T_2(t).a$, $T_1(t).b$, et $T_2(t).b$, et sont décrites sur la Figure IV.3.10. D'après les conditions d'états stationnaires, les températures sont constantes jusqu'à l'occurrence de la *défaillance totale* de la pompe au temps $t = 30$ secondes, puis elles croissent en fonction des Équations IV.3.16 à IV.3.21 et, une fois le SCRAM activé au temps $t = 36$ secondes, décroissent après un certain délai. À noter que les températures du sodium sont quasi égales entre elles avant l'activation du SCRAM (la différence entre $T_1(t)$ et $T_2(t)$ est inférieure à 0.02 K avant la *défaillance totale* de la pompe, et ensuite cette différence augmente). Une fois le SCRAM activé, $T_1(t)$ décroît plus rapidement que $T_2(t)$.

Les évolutions du flux de sodium ($G(t)$) dans les scénarios c, d, et e, sont respectivement notées $G(t).c$, $G(t).d$, et $G(t).e$, et sont décrites sur la Figure IV.3.11. D'après les Équations IV.3.16 et IV.3.17, et les déviations aléatoires du couple de la pompe définies par l'Équation IV.3.31, le flux décroît aléatoirement dans ces trois scénarios et, par conséquent, les courbes obtenues pour ces trois cas sont différentes.

Les évolutions des températures du sodium ($T_1(t)$ et $T_2(t)$) dans les scénarios c, d, et e, sont respectivement notées $T_1(t).c$, $T_2(t).c$, $T_1(t).d$, $T_2(t).d$, $T_1(t).e$, et $T_2(t).e$, et sont décrites sur la Figure IV.3.12. D'après les Équations IV.3.16 à IV.3.21, et les déviations aléatoires du couple de la pompe définies par l'Équation IV.3.31, les températures croissent aléatoirement dans ces trois scénarios. À noter que les températures du sodium sont quasi égales entre elles avant l'activation du SCRAM (la

différence entre $T_1(t)$ et $T_2(t)$ augmente globalement en fonction du temps, mais cette différence est inférieure à *1.00* K pour, au moins, $t \leq 90$ secondes).

IV.3.3.2.4. Analyses de fiabilité

Afin d'effectuer des analyses de fiabilité, un domaine de sécurité *D* doit être défini. Pour ce cas d'étude, ce domaine dépend logiquement des températures du sodium dans les canaux ($T_1(t)$ et $T_2(t)$), et sa frontière est ici définie par $T_D = 933$ K. Cependant, d'après les scénarios a et b présentés dans la Section IV.3.3.2.3, il est montré que, dans le cas d'une *défaillance totale* de la pompe, les températures du sodium croissent si rapidement que, même si la fonction de sécurité est convenablement réalisée, la frontière T_D peut être dépassée durant quelques secondes. La définition du domaine de sécurité *D* est donc complétée par une condition de temps, et il est alors considéré qu'un *évènement dangereux* se produit si et seulement si au moins une des températures du sodium ($T_1(t)$ ou $T_2(t)$) est égale ou supérieure à $T_D = 933$ K pour une durée supérieure à *5* secondes.

La fonction de sécurité est quant à elle définie d'après les valeurs seuils de température du sodium (T_{max}), et du flux (G_{min}), qui doivent commander l'activation du SCRAM. Pour ce cas d'étude, les valeurs $T_{max} = 923$ K et $G_{min} = 3\,345$ kg·m^{-2}·s^{-1} sont utilisées. Par exemple, dans les scénarios a et b présentés dans la Section IV.3.3.2.3, une fois qu'une *défaillance totale* de la pompe se produit, ces deux valeurs seuils sont atteintes presqu'en même temps au bout d'environ *6* secondes. Dans les scénarios c, d, et e, il est montré que, lorsque la pompe est dans un état *dégradé*, la valeur seuil de température est atteinte en premier (au bout d'un temps aléatoire, selon les déviations du couple de la pompe), puis la valeur seuil du flux est atteinte approximativement *2* à *5* secondes plus tard. Dans ces exemples, le scénario c correspond à un cas où le SCRAM est activé dès la valeur seuil de température atteinte, et le scénario d à un cas où le SCRAM n'est activé qu'une fois la valeur seuil du flux atteinte (par exemple, dans le cas d'une *défaillance dangereuse* des deux capteurs-transmetteurs de température).

Puisque les composants du système ont des états possibles de *défaillance sûre* (et les capteurs-transmetteurs de température ont également des états possibles de *dérives sûres*), il est aussi possible que les valeurs seuils soient « détectées », bien que les températures et le flux n'aient pas, en réalité, dépassées les valeurs seuil. Le SCRAM peut alors être activé à tors, ce qui implique un *déclenchement intempestif*. Parce que les capteurs-transmetteurs de température peuvent être sujets à des *dérives*, il est cependant probablement inapproprié de compter comme un *déclenchement intempestif* un scénario où le SCRAM est activé à seulement quelques degrés au dessous de la valeur seuil de température. Pour ce cas d'étude, un *déclenchement intempestif* est donc considéré si et seulement si le SCRAM est activé tandis que les deux températures du sodium sont inférieures à $T_{max} - 5$ K = *918* K.

Lorsque ni un *évènement dangereux* ni un *déclenchement intempestif* ne s'est produit, le système est en vie « utile ». Au cours de cette période, si le SCRAM est activé tandis qu'au moins une température du sodium est supérieure à $T_{max} - 5$ K = *918* K, mais qu'aucune température du sodium n'a dépassé $T_D = 933$ K durant plus de *5* secondes, alors une *activation sous-contrôle* est considérée. Pour résumer, les trois scénarios possibles (*évènement dangereux*, *déclenchement intempestif*, et *activation sous-contrôle*) sont classés selon les critères donnés dans le Tableau IV.3.8.

Les analyses de fiabilité sont effectuées d'après un évènement initiateur qui est l'occurrence d'un état *dégradé* de la pompe ($SPM(t) = 3$), c'est-à-dire le premier évènement dangereux faisant sortir les variables du processus de leurs états stationnaires. Au temps $t = t_0$, les composants du système

sont donc dans des états *opérants* (toutes les variables d'état des composants sont égales à *1*), excepté pour la pompe qui est dans un état *dégradé* ($SPM(t_0) = 3$) ; les variables du processus sont dans les conditions initiales données dans le Tableau IV.3.5 ; les variables d'information pour les résultats de mesure et les signaux sont définies par les Équations IV.3.22 à IV.3.26, et les autres variables d'information sont égales à *0.0* ; et les variables de déviation sont égales à *0.0*.

Afin d'évaluer les effets des « fonctionnalités intelligentes » des capteurs-transmetteurs, plusieurs cas sont analysés selon la valeur de α_{ref} (cf. Section IV.3.3.1.4). Lorsque $\alpha_{ref} = +\infty$, les paramètres de correction des dérives $T_1^c(t)$ et $T_2^c(t)$ sont toujours égaux à *0.0*, d'après leurs valeurs au temps $t = t_0$ et le Tableau IV.3.7, c'est-à-dire qu'aucune correction des dérives n'est considérée. Autrement, plus la valeur de α_{ref} est faible, et plus les paramètres de correction des dérives sont sujets à des « réajustements », d'après les règles données dans le Tableau IV.3.7. Les analyses ont été effectuées d'après *100 000* simulations de Monte Carlo, pour $\alpha_{ref} = +\infty$, $\alpha_{ref} = 5.0$, $\alpha_{ref} = 3.0$, $\alpha_{ref} = 1.0$, et $\alpha_{ref} = 0.5$. Les pourcentages respectifs obtenus pour chaque type de scénario (*évènement dangereux*, *déclenchement intempestif*, et *activation sous-contrôle*) sont donnés dans le Tableau IV.3.9, et les temps moyens respectifs de vie « utile » sont donnés dans le Tableau IV.3.10.

Le Tableau IV.3.9 montre que l'utilisation des « fonctionnalités intelligentes » des capteurs-transmetteurs permet une plus grande proportion d'*activations sous-contrôle*, en réduisant la proportion de *déclenchements intempestifs*. En effet, les corrections des dérives compensent les *dérives sûres* (positives) des capteurs-transmetteurs de température, qui sont d'importants contributeurs de *déclenchements intempestifs*. En revanche, la proportion d'*évènements dangereux* n'est pas réduite par les corrections des dérives, notamment parce que même en cas de *dérives dangereuses* (négatives) des capteurs-transmetteurs de température, le SCRAM peut toujours être activé de par la détection d'un seuil bas du flux de sodium (la mesure du flux agit comme une redondance pour la fonction de sécurité). Il peut même être observé que l'utilisation des corrections des dérives augmente légèrement la proportion d'*évènements dangereux*. Ceci est une conséquence directe de la réduction des *déclenchements intempestifs*. En effet, en prévenant l'occurrence de *déclenchements intempestifs*, le temps de vie « utile » du système est prolongé, comme montré dans le Tableau IV.3.10, et les *évènements dangereux* sont automatiquement plus probables car les probabilités d'occurrence de *défaillances dangereuses* augmentent avec le temps.

Lorsque des corrections des dérives sont utilisées, le choix du paramètre α_{ref} affecte alors les performances du système selon des relations non-monotones. Au regard des critères des *activations sous-contrôle*, des *déclenchements intempestifs*, et des temps moyens de vie « utile », une valeur optimale de α_{ref} peut être trouvée aux alentours de *1.0*, d'après les cas donnés dans le Tableau IV.3.9. En effet, lorsque le paramètre α_{ref} est plus petit, les corrections des dérives sont plus sensibles, et la probabilité d'accepter une mauvaise hypothèse parmi les règles données dans le Tableau IV.3.7 augmente. En particulier, des résultats de mesure corrects peuvent alors être biaisés par des paramètres de correction des dérives qui sont définis d'après des résultats de mesure incorrects (notamment dans les cas de défaillances multiples, par exemple lorsqu'à la fois un capteur-transmetteur de température et le capteur-transmetteur de flux ne sont pas dans des états *opérants*).

IV.3.3.3. Conclusions partielles et perspectives

Afin de prendre en compte les particularités des CTI, le formalisme mathématique de la fiabilité dynamique a été étendu en introduisant des variables d'information. De plus, des variables de déviation ont été utilisées pour modéliser des erreurs comme des dérives de certains composants du

Tableau IV.3.8. Classification des scénarios

scénario	critères
évènement dangereux	$T_1(t) \geq T_D$ ou $T_2(t) \geq T_D$ durant plus de *5* secondes, avec $T_D = 933$ K
déclenchement intempestif	$T_1(t) < T_{max} - 5$ K et $T_2(t) < T_{max} - 5$ K lorsque le SCRAM devient activé, avec $T_{max} = 923$ K
activation sous-contrôle	autres cas i.e. $T_1(t) \geq T_{max} - 5$ K ou $T_2(t) \geq T_{max} - 5$ K lorsque le SCRAM devient activé, et ni $T_1(t) \geq T_D$ ni $T_2(t) \geq T_D$ durant plus de *5* secondes

Tableau IV.3.9. Résultats des analyses de fiabilité : répartition[a] des scénarios

scénario	$\alpha_{ref} = +\infty$	$\alpha_{ref} = 5.0$	$\alpha_{ref} = 3.0$	$\alpha_{ref} = 1.0$	$\alpha_{ref} = 0.5$
évènement dangereux (± *0.09*)[b]	*2.4*	*3.4*	*3.2*	*3.4*	*3.2*
déclenchement intempestif (± *0.26*)[b]	*51.5*	*47.8*	*44.5*	*44.0*	*44.2*
activation sous-contrôle (± *0.26*)[b]	*46.1*	*48.8*	*52.3*	*52.7*	*52.5*

[a]Ces résultats ont été obtenus d'après *100 000* simulations de Monte Carlo pour chaque colonne.
[b]Intervalle de confiance à *90*%, autours des moyennes données dans ce tableau, en faisant l'hypothèse que les résultats suivent des distributions Binomiales, et en les approximant par des distributions Normales.

Tableau IV.3.10. Résultats des analyses de fiabilité : temps moyens[a] de vie « utile » [seconde]

scénario	$\alpha_{ref} = +\infty$	$\alpha_{ref} = 5.0$	$\alpha_{ref} = 3.0$	$\alpha_{ref} = 1.0$	$\alpha_{ref} = 0.5$
temps moyen de vie « utile » (± *0.09*)[b]	*48.86*	*51.32*	*51.57*	*51.63*	*51.57*

[a]Ces résultats ont été obtenus d'après *100 000* simulations de Monte Carlo pour chaque colonne.
[b]Intervalle de confiance à *90*%, autours des moyennes données dans ce tableau, en faisant l'hypothèse que les résultats suivent des distributions Normales.

système. Une approche formalisée en réseau de Petri a ensuite été proposée afin de modéliser, simuler, et analyser la fiabilité dynamique de tels systèmes. Pour cela, des méthodes numériques ont été utilisées, basées sur des développements de Taylor et des différences finies. En suivant ce formalisme, il a notamment été possible de proposer un modèle générique pour CTI, et de modéliser et analyser efficacement un cas d'étude relativement complet.

Le cas d'étude est composé de *8* variables d'état des composants, pour un nombre total de $3^6 \cdot 5^2 = 18\,225$ états possibles (d'après le Tableau IV.3.2) ; *13* variables du processus, bien que seulement *2* d'entre elles soient directement affectées par des variables d'autres types (la vitesse angulaire de la pompe et la puissance générée par le cœur du réacteur) et pourraient donc théoriquement être utilisées pour exprimer exhaustivement toutes les autres variables du processus ; *13* variables d'information, dont *3* sont binaires et *10* sont continues ; et *3* variables de déviation. En utilisant une discrétisation de chaque variable continue par un nombre *m* d'états, le nombre total d'états qui décrit le système complet est : $3^6 \cdot 5^2 \cdot m^2 \cdot 2^3 \cdot m^{10} \cdot m^3$, à chaque instant *t*. Même pour une faible valeur de *m*, par exemple pour $m = 16$ (ce qui n'est certainement pas suffisant pour permettre d'effectuer des analyses correctes du système), le nombre total d'états du système atteint $1.68 \cdot 10^{23}$, ce qui est sans doute plus que le nombre de grains de sable sur toutes les plages et les déserts de la Terre, et le nombre d'étoiles dans l'univers connu [CNN03]. Malgré ce nombre très important d'états, le système complet a été modélisé en utilisant un réseau de Petri qui, en utilisant le formalisme proposé, est formé d'un nombre de places et de transitions qui sont tous deux égaux au nombre de variables du système (en incluant le temps *t*), c'est-à-dire *38*, plus le nombre de places et de transitions utilisés dans les méta-transitions pour les variables du processus et de déviation, c'est-à-dire *16*, pour un total de *54*.

Parce que la taille du modèle est linéairement dépendante du nombre de variables (et non du nombre d'interactions et/ou d'états), il n'y a pas vraiment de problème d'échelle pour modéliser des systèmes plus complexes. Cependant, le temps nécessaire à l'exécution des simulations, et aux analyses, est un autre défi. En effet, bien qu'un logiciel comme CPN Tools soit assez flexible pour répondre aux principales exigences du formalisme proposé, il n'est pas optimisé pour réaliser ces tâches, qui nécessitent alors des temps d'exécution relativement longs. Pour le cas d'étude présenté, le temps nécessaire à la simulation d'un scénario, en utilisant ce logiciel, est d'environ quatre secondes avec un microprocesseur de *2,20* GHz. Des tests empiriques effectués avec d'autres outils, encore expérimentaux, ont cependant montré que ces temps de simulation pouvaient être réduits par un facteur d'ordre 10^2 à 10^3 avec l'utilisation d'un logiciel dédié à ces analyses. Le développement d'un tel outil est donc une étape importante pour une large diffusion de l'approche proposée.

Finalement, on peut conclure que l'approche présentée fournit un moyen de modélisation et d'analyse de systèmes complexes, en particulier de SCC incluant des CTI, capable de faire face à des problèmes de grande échelle, tout en offrant des flexibilités de modélisation et une interface graphique. De tels critères pour une plateforme de fiabilité dynamique, dans le contexte des évaluations probabilistes des risques (EPR), ont été présentés et discutés par P.E. Labeau *et al.* [PLa00]. Le formalisme proposé peut alors apporter certains éléments de réponse aux problématiques soulevées pour le développement d'un tel outil. Parmi les possibilités d'optimisation des performances d'analyses, des améliorations des méthodes de Monte Carlo utilisées seraient souhaitables, par exemple en utilisant des techniques de biais et/ou des incréments de temps adaptatifs. En réduisant les temps de simulation, des analyses d'incertitudes seraient alors envisageables. D'autres perspectives de développement concernent l'intégration de travaux connexes, notamment sur la fiabilité des logiciels, la sûreté de fonctionnement des réseaux de communication, et sur les opérations humaines (fiabilité et facteur humain), ainsi que des procédures formelles d'intégration de ces approches dans les EPR.

CHAPITRE V

CONCLUSIONS ET PERSPECTIVES

Ce chapitre présente des conclusions et des perspectives générales des travaux de thèses relatés dans ce mémoire.

SOMMAIRE DU CHAPITRE V

V.1. CONCLUSIONS ET PERSPECTIVES

Une partie des travaux de thèse présentés dans ce mémoire a concerné l'évaluation de la sûreté de fonctionnement de systèmes relatifs à la sécurité en général. Sur la base d'une approche « analytique » et d'une méthodologie combinant des aspects quantitatifs et qualitatifs, les outils proposés permettent d'évaluer des critères de sûreté de fonctionnement (probabilités qu'un système soit capable d'accomplir une fonction) en tenant compte de certaines propriétés des systèmes (architectures, taux de défaillance), des politiques de maintenance (tests de révision partiels et complets), et des facteurs d'influence (incluant notamment des conditions environnementales et opérationnelles des systèmes). Ceux-ci ont ainsi permis d'apporter quelques éléments pour contribuer au développement de modèles d'évaluation probabiliste des risques qui soient cohérents (par des résultats gradués en fonction des informations relatives à la sécurité), consistants (par l'intégration d'un plus grand nombre d'informations), mais également relativement simples à exploiter (grâce à des expressions générales et à une méthodologie globale). De plus amples développements pourront également étendre les modèles proposés (par exemple, pour des systèmes plus hétérogènes et d'architectures plus générales, des politiques de tests plus hétéroclites), notamment afin d'y intégrer davantage d'informations relatives à la sécurité (par exemple, causes communes de défaillance, phénomènes de vieillissement, maintenances imparfaites, facteurs humains et organisationnels). Ces futurs travaux pourront vraisemblablement tirer avantage d'une intégration de modèles fondés à la fois sur des bases qualitatives et quantitatives, par exemple en utilisant des approches bayésiennes et issues de la théorie de l'information [CSh49].

La majeure partie de la thèse a été consacrée à l'évaluation de la sûreté de fonctionnement de capteurs-transmetteurs à fonctionnalités numériques, communément qualifiés de « capteurs-transmetteurs intelligents » (CTI), et aux systèmes de contrôle-commande (SCC) intégrant des CTI. En considérant tout d'abord un CTI seul, une modélisation a été proposée afin de représenter les fonctions du système, les éléments matériels, les défauts et défaillances, ainsi que les diverses relations entre ces éléments. Par l'introduction d'évènements de relations (par exemple, pour représenter la probabilité que l'état défaillant d'un élément matériel implique le dysfonctionnement d'une certaine fonction), il a ensuite été possible d'évaluer les probabilités de dysfonctionnements et de modes de défaillance (définis par combinaisons des fonctions) du système, en y intégrant les interactions internes (matérielles et fonctionnelles), ainsi que les comportements difficiles à appréhender. Des analyses d'incertitudes, à la fois liées aux paramètres (notamment de par le peu de retour d'expérience disponible) et au modèle (notamment de par les comportements mal connus du système en cas de défauts ou de défaillances), ont alors montré que, dans la plupart des cas, ces évaluations étaient relativement robustes (les incertitudes dans les résultats sont souvent moins grandes que les incertitudes dans les données d'entrée). Ces propriétés rendent l'approche proposée plutôt prometteuse pour des analyses de fiabilité de systèmes à fonctionnalités numériques. Il serait notamment intéressant d'appliquer de telles analyses à des systèmes de plus grande échelle, et à plus forte présence d'unités programmées et de logiciels, afin de vérifier le potentiel escompté. Certains développements pourraient également chercher à prendre en compte plus explicitement les aspects logiciels dans cette approche. De plus, plusieurs analyses structurelles et fonctionnelles pourraient être mises en place sur la base de la modélisation proposée, et des relations stochastiques entre défauts et défaillances, éléments matériels, et fonctions des systèmes.

Les derniers travaux de thèse ont considéré les CTI en tant qu'éléments de SCC. Une approche étendue de fiabilité dynamique a alors été développée afin de modéliser explicitement les interactions entre CTI, les interactions avec les autres éléments du système, ainsi que celles avec le processus contrôlé. Une première contribution a alors été d'intégrer des variables d'information

(incluant notamment les informations manipulées par les CTI), et de déviation (par exemple, pour représenter des phénomènes de dégradations et de dérives), dans un formalisme de fiabilité dynamique, afin de prendre en compte les particularités des CTI. Ensuite, une modélisation basée sur des réseaux de Petri a été proposée, qui est relativement flexible et facile à manipuler, et qui permet d'effectuer des analyses de fiabilité par simulations de Monte Carlo, sur la base de méthodes numériques. Parmi les premiers développements envisageables de cette approche, figurent l'intégration explicite d'opérations humaines (avec des caractéristiques qui leurs sont propres) et de la sûreté de fonctionnement liée à la communication entre les éléments du système, ainsi que l'optimisation des méthodes de simulations, notamment afin de permettre d'effectuer, par la suite, des analyses d'incertitudes.

Il n'est probablement pas pertinent de conclure ici sur le niveau de fiabilité offert par les capteurs-transmetteurs à fonctionnalités numériques, par rapport à des systèmes plus « basiques ». Ces considérations sont en effet dépendantes de nombreux facteurs à la fois matériels (par exemple, liés à la fiabilité des éléments sensibles d'un capteur, et à celle des unités de traitement) et humains (par exemple, liés à l'exploitation du système, et à la gestion de la maintenance), où l'implication des fonctionnalités numériques est vraisemblablement plus sujette à des problèmes de conception et d'utilisation qu'à leurs propriétés intrinsèques, ce qui exclut les possibilités de généraliser d'éventuelles conclusions en termes de fiabilité. De plus, face au développement rapide des nouvelles technologies, les facteurs intervenant dans la fiabilité des systèmes sont en constante évolution, et les comparaisons exhaustives de différentes générations de systèmes sont souvent illusoires.

Laissant donc ici la fiabilité de côté, les travaux réalisés au cours de cette thèse ont néanmoins permis de faire ressortir quelques tendances relatives aux critères de disponibilité (absence de défaillance) et de sécurité (absence de défaillance « dangereuse »), que ce soit pour les CTI considérés isolément, ou en tant qu'éléments de SCC. Au cœur des fonctionnalités numériques, se trouve en effet les autodiagnostics (surveillances de paramètres internes et externes, détections de défauts et de défaillances). Sur la base des informations ainsi obtenues, si l'état ou l'environnement d'un système est jugé « inapproprié » (par exemple, par la détection d'un défaut ou d'une défaillance), deux options sont alors envisageables : soit procéder à une « mise en position de repli en sécurité » du système, c'est-à-dire activer la fonction de sécurité pour laquelle il est destiné (la défaillance devient alors « sûre ») ; soit procéder à des « remises en état opérationnel », par exemple par des corrections d'erreurs de mesure, des auto-ajustages, ou des reconfigurations en ligne. Si la première option privilégie la sécurité (à condition bien sûr que la « position de repli » soit effectivement « sûre »), la seconde option privilégie la disponibilité en prévenant des déclenchements intempestifs de la fonction de sécurité. Cependant, les sollicitations de « remises en état opérationnel » peuvent, dans certains cas, ne pas conduire à la situation escomptée (en laissant le système dans le même état, ou en provoquant un autre état de défaillance) et, possiblement, faire passer le système d'un état de « défaillance détectée » (celui qui est à l'initiative de la sollicitation de « remise en état ») à un état de « défaillance non détectée ». Cette mise en balance de la disponibilité avec la sécurité peut alors être observée à l'échelle des CTI, mais également à l'échelle des SCC intégrant de tels CTI. En proposant des modèles d'évaluation de ces systèmes, les travaux présentés dans ce mémoire de thèse offrent ainsi certains éléments pour contribuer au développement d'outils permettant d'effectuer les choix les plus adéquats en termes de maîtrise des risques.

V.2. QUELQUES MOTS POUR CLÔTURER CE MÉMOIRE

Pour clore ce mémoire de thèse, nous proposons de revenir ici en quelques mots sur les aspects principaux qui ont motivé la réalisation de cette thèse, à savoir, la contribution au développement de modèles d'évaluation probabiliste des risques, dans le contexte de la maîtrise des risques technologiques en France.

En effet, force est de constater le décalage important entre le développement rapide de nouvelles technologies, répondant généralement à de fortes contraintes économiques, humaines, et environnementales, et celui de la maîtrise des risques technologiques. Un exemple éloquent est celui de la réglementation française sur la prévention des risques industriels, qui n'a intégré des critères probabilistes qu'à partir de 2003, c'est-à-dire près de trente ans après le développement des premières évaluations probabilistes des risques, notamment dans le domaine du nucléaire. De par l'essence même d'un risque, seule une approche probabiliste apparaît en effet appropriée, et l'évaluation probabiliste des risques est alors un préalable à celle de la maîtrise des risques. En 2010, la dimension « aléatoire » du risque n'est cependant pas toujours convenablement intégrée, comme le montre les amalgames répandus entre « probabilité » et « fréquence », ainsi que les préconisations de certaines approches dites « semi-quantitatives », et parfois même uniquement qualitatives. C'est néanmoins sur la base de ces évaluations que sont réalisés des études de dangers (EDD) et des plans de prévention des risques technologiques (PPRT), à partir desquels sont mises en place des actions sur l'urbanisme, pouvant conduire jusqu'à des expropriations, ou au contraire autoriser (ou maintenir) la présence d'établissements privés ou publics dans certaines zones. Tandis que le développement exponentiel des technologies (que nous pourrions peut-être tout simplement qualifier de « développement humain ») semble être associé à une croissance du même ordre des dangers potentiels pour les êtres humains et l'environnement, une préoccupation notable est alors la divergence avec la mise en place des outils appropriés à la maîtrise des risques. De plus, les avancées majeures en termes de maîtrise des risques ne semblent malheureusement que se produire de façon ponctuelle, principalement à la suite d'accidents à forte retombée médiatique (notamment, Seveso en 1976, Three Mile Island en 1979, AZF en 2001 [ALa08]). Indubitablement, un des défis du Développement Durable est de modifier cette tendance afin de mettre en adéquation les outils de maîtrise des risques avec le développement des nouvelles technologies.

Les travaux de thèse présentés dans ce mémoire se sont alors inscrits dans cette mouvance en cherchant à contribuer au développement de modèles d'évaluation probabiliste des risques, et notamment face à certaines problématiques liées aux nouvelles technologies. Plusieurs modèles ont alors été proposés, afin d'évaluer la sûreté de fonctionnement de systèmes relatifs à la sécurité, cherchant au mieux à intégrer des informations pertinentes pour la sécurité (relatives aux systèmes, à son environnement, et à son utilisation), et plus particulièrement pour des systèmes à fonctionnalités numériques, en tenant compte des interactions internes (fonctionnelles et matérielles) et externes (avec d'autres éléments, et les processus contrôlés). Les travaux présentés dans ce mémoire de thèse ont été développés dans le souci d'être techniquement exploitables en milieu industriel. La réalisation et la mise à disposition d'outils informatiques permettant d'exploiter ces modèles donneraient alors la possibilité de mener à bien des évaluations de risques plus complètes et plus abouties dans le cadre des EDD, puis des PPRT. L'intégration de ces approches dans une démarche plus globale d'évaluation offrirait, de plus, d'intéressantes perspectives pour améliorer la maîtrise des risques, notamment en ce qui concerne la pertinence et l'efficacité des prises de décision.

La mise en œuvre effective de la maîtrise des risques technologiques, basée sur des évaluations probabilistes adaptées aux besoins (et en constante évolution), nécessite cependant des travaux de recherche et de développement bien plus larges. En particulier, la formalisation de modèles d'évaluation probabiliste, construits sur des bases scientifiquement solides, semble être un des premiers impératifs, afin notamment de mettre en place des évaluations de risques technologiques qui soient rigoureuses, justes, et cohérentes à l'échelle de l'industrie française, et européenne.

CHAPITRE VI

ANNEXES

Ce chapitre regroupe les annexes où figurent les démonstrations de plusieurs expressions mathématiques présentées dans les chapitres précédents.

SOMMAIRE DU CHAPITRE VI

VI.1. ANNEXES AU CHAPITRE II

VI.1.1. Preuves de l'Équation II.1.1

D'après les notations présentées dans la Section II.1.2.2, le diagramme de fiabilité de la Figure II.1.2, et les règles de la théorie de la fiabilité applicables à une structure série [MRa02] :

$$A_e(t) = e^{-E\cdot\lambda\cdot(t-t_{i-1})}\cdot e^{-(1-E)\cdot\lambda\cdot t} \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.1]}$$

$$A_e(t) = e^{E\cdot\lambda\cdot t_{i-1}}\cdot e^{-\lambda\cdot t} \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.2]}$$

VI.1.2. Preuves des Équations II.1.2 et II.1.3

D'après l'Équation VI.1.2, les notations présentées dans la Section II.1.2.2, et les règles de la théorie de la fiabilité applicables à des structures *M*oo*N* (en anglais, « *k-out-of-n* » avec *k* = *M* et *n* = *M*) [MRa02] :

$$A(t) = \sum_{k=M}^{N}\left[\ \binom{N}{k}\cdot A_e(t)^k\cdot\left(1-A_e(t)\right)^{N-k}\ \right] \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.3]}$$

$$A(t) = \sum_{k=M}^{N}\left[\ \binom{N}{k}\cdot e^{k\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-k\cdot\lambda\cdot t}\cdot\left(1-e^{E\cdot\lambda\cdot t_{i-1}}\cdot e^{-\lambda\cdot t}\right)^{N-k}\ \right] \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.4]}$$

En utilisant la formule du binôme de Newton, il est possible d'obtenir la décomposition suivante :

$$A(t) = \sum_{k=M}^{N}\left[\ \binom{N}{k}\cdot e^{k\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-k\cdot\lambda\cdot t}\cdot\sum_{l=0}^{N-k}\left[\ \binom{N-k}{l}\cdot(-1)^{N-k-l}\cdot\left(e^{(N-k-l)\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-(N-k-l)\cdot\lambda\cdot t}\right)\ \right]\ \right]$$
$$\text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.5]}$$

$$A(t) = \sum_{k=M}^{N}\sum_{l=0}^{N-k}\left[\ \binom{N}{k}\cdot\binom{N-k}{l}\cdot(-1)^{N-k-l}\cdot e^{(N-l)\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-(N-l)\cdot\lambda\cdot t}\ \right]$$
$$\text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.6]}$$

D'après le théorème de Fubini, il est possible de permuter ainsi l'ordre des sommes :

$$A(t) = \sum_{l=0}^{N-M}\sum_{k=M}^{N-l}\left[\ \binom{N}{k}\cdot\binom{N-k}{l}\cdot(-1)^{N-k-l}\cdot e^{(N-l)\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-(N-l)\cdot\lambda\cdot t}\ \right]$$
$$\text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.7]}$$

Avec le changement de variable $x = N - l$, puis un artifice de calcul :

$$A(t) = \sum_{x=M}^{N}\sum_{k=M}^{x}\left[\ \binom{N}{k}\cdot\binom{N-k}{N-x}\cdot(-1)^{x-k}\cdot e^{x\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-x\cdot\lambda\cdot t}\ \right] \qquad \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.8]}$$

$$A(t) = \sum_{x=M}^{N}\sum_{k=M}^{x}\left[\ \binom{N}{k}\cdot\binom{N-k}{N-x}\cdot\frac{x!}{x!}\cdot(-1)^{x-k}\cdot e^{x\cdot E\cdot\lambda\cdot t_{i-1}}\cdot e^{-x\cdot\lambda\cdot t}\ \right] \text{pour } t_{i-1} \le t < t_i \qquad \text{[VI.1.9]}$$

$$A(t) = \sum_{x=M}^{N} \sum_{k=M}^{x} \left[\binom{N}{x} \cdot \binom{x}{k} \cdot (-1)^{x-k} \cdot e^{x \cdot E \cdot \lambda \cdot t_{i-1}} \cdot e^{-x \cdot \lambda \cdot t} \right] \quad \text{pour } t_{i-1} \leq t < t_i \quad [VI.1.10]$$

Finalement :

$$A(t) = \sum_{x=M}^{N} \left[S(M,N,x) \cdot e^{x \cdot E \cdot \lambda \cdot t_{i-1}} \cdot e^{-x \cdot \lambda \cdot t} \right] \quad \text{pour } t_{i-1} \leq t < t_i \quad [VI.1.11]$$

avec :

$$S(M,N,x) = \sum_{k=M}^{x} \left[\binom{N}{x} \cdot \binom{x}{k} \cdot (-1)^{x-k} \right] \quad \text{pour } x = M, \ldots, N \quad [VI.1.12]$$

VI.1.3. Preuves de l'Équation II.1.4

D'après l'Équation VI.1.11, les notations présentées dans la Section II.1.2.2, et les hypothèses présentées dans la Section II.1.2.1 :

$$PFD_i = \frac{1}{T_i} \cdot \int_{t_{i-1}}^{t_i} U(t) \cdot dt \quad [VI.1.13]$$

$$PFD_i = 1 - \frac{1}{T_i} \cdot \int_{t_{i-1}}^{t_i} A(t) \cdot dt \quad [VI.1.14]$$

$$PFD_i = 1 - \frac{1}{T_i} \cdot \int_{t_{i-1}}^{t_i} \sum_{x=M}^{N} \left[S(M,N,x) \cdot e^{x \cdot E \cdot \lambda \cdot t_{i-1}} \cdot e^{-x \cdot \lambda \cdot t} \right] \cdot dt \quad [VI.1.15]$$

$$PFD_i = 1 - \sum_{x=M}^{N} \left[S(M,N,x) \cdot e^{-x \cdot (1-E) \cdot \lambda \cdot t_{i-1}} \cdot \frac{1 - e^{-x \cdot \lambda \cdot T_i}}{x \cdot \lambda \cdot T_i} \right] \quad [VI.1.16]$$

VI.1.4. Preuves de l'Équation II.1.5

D'après l'Équation VI.1.16, les notations présentées dans la Section II.1.2.2, et les hypothèses présentées dans la Section II.1.2.1 :

$$PFD_{avg} = \frac{1}{\tau} \cdot \sum_{i=1}^{n} \left[T_i \cdot PFD_i \right] \quad [VI.1.17]$$

$$PFD_{avg} = 1 - \sum_{x=M}^{N} \left[S(M,N,x) \cdot \sum_{i=1}^{n} \left[e^{-x \cdot (1-E) \cdot \lambda \cdot t_{i-1}} \cdot \frac{1 - e^{-x \cdot \lambda \cdot T_i}}{x \cdot \lambda \cdot \tau} \right] \right] \quad [VI.1.18]$$

VI.2. ANNEXES AU CHAPITRE III

VI.2.1. Preuves de l'Équation III.3.1

D'après les notations présentées dans la Section III.3.1.2, et l'arbre de défaillance équivalent à une porte « continue » de la Figure III.3.2 :

$$P[\text{sommet}](t) = P[(\bigcup_{j=1,\dots,N} (E_j \cap P_j)) \cup (\bigcap_{i=1,\dots,N} E_i)] \quad [VI.2.1]$$

L'utilisation des lois de probabilités, et notamment celles des probabilités conditionnelles, permet alors d'obtenir les expressions suivantes :

$$P[\text{sommet}](t) = P[\bigcup_{j=1,\dots,N} (E_j \cap P_j)] + P[\bigcap_{i=1,\dots,N} E_i] - P[(\bigcup_{j=1,\dots,N} (E_j \cap P_j)) \cap (\bigcap_{i=1,\dots,N} E_i)] \quad [VI.2.2]$$

$$P[\text{sommet}](t) = P[\bigcup_{j=1,\dots,N} (E_j \cap P_j)] + P[\bigcap_{i=1,\dots,N} E_i] - P[\bigcap_{i=1,\dots,N} E_i] \cdot P[(\bigcup_{j=1,\dots,N} (E_j \cap P_j)) \mid (\bigcap_{i=1,\dots,N} E_i)] \quad [VI.2.3]$$

$$P[\text{sommet}](t) = P[\bigcup_{j=1,\dots,N} (E_j \cap P_j)] + P[\bigcap_{i=1,\dots,N} E_i] - P[\bigcap_{i=1,\dots,N} E_i] \cdot P[\bigcup_{j=1,\dots,N} P_j] \quad [VI.2.4]$$

$$P[\text{sommet}](t) = P[\bigcup_{j=1,\dots,N} (E_j \cap P_j)] + P[\bigcap_{i=1,\dots,N} E_i] \cdot (1 - P[\bigcup_{j=1,\dots,N} P_j]) \quad [VI.2.5]$$

$$P[\text{sommet}](t) = P[\bigcup_{j=1,\dots,N} (E_j \cap P_j)] + P[\bigcap_{i=1,\dots,N} E_i] \cdot P[\bigcap_{j=1,\dots,N} P_j^*] \quad [VI.2.6]$$

avec P_j^* qui représente la non-occurrence de l'évènement P_j.

Finalement :

$$P[\text{sommet}](t) = 1 - \prod_{i=1,\dots,N} (1 - p_i \cdot P[E_i](t)) + \prod_{i=1,\dots,N} ((1 - p_i) \cdot P[E_i](t)) \quad [VI.2.7]$$

VI.2.2. Preuves de l'Équation III.3.4

Soient U et V deux variables aléatoires dont la densité de probabilité conjointe est $f_{U,V}(u, v)$, alors la densité de probabilité de la variable aléatoire $W = U \cdot V$ est [VRo76] :

$$f_W(w) = f_{U \cdot V}(w) = \int_{-\infty}^{+\infty} f_{U,V}(u, w / u) \cdot (1 / abs(u)) \cdot du \quad [VI.3.8]$$

avec $abs(u)$ qui représente la valeur absolue de u.

Si les variables aléatoires U et V sont indépendantes, et dont les densités de probabilités sont respectivement $f_U(u)$ et $f_V(v)$, alors :

$$f_W(w) = f_{U \cdot V}(w) = \int_{-\infty}^{+\infty} f_U(u) \cdot f_V(w / u) \cdot (1 / abs(u)) \cdot du \quad [VI.3.9]$$

De plus, si les variables aléatoires U et V décrivent des valeurs de probabilité, alors, d'après les Équations III.3.2 et III.3.3 :

$$f_W(w) = f_{U \cdot V}(w) = \int_{0}^{1} f_U(u) \cdot f_V(w / u) \cdot (1 / u) \cdot du \quad [VI.3.10]$$

VI.2.3. Preuves de l'Équation III.3.5

Soit U une variable aléatoire qui décrit une valeur de probabilité, et dont la densité de probabilité est $f_U(u)$, alors la densité de probabilité de la variable aléatoire $R = 1 - U$ est :

$$f_R(r) = f_{1-U}(r) = f_U(1 - r) \qquad \text{[VI.3.11]}$$

Soit V une autre variable aléatoire qui décrit une valeur de probabilité, dont la densité de probabilité est $f_V(v)$, et qui est indépendante de la variable aléatoire U, alors la densité de probabilité de la variable aléatoire $S = (1 - U) \cdot (1 - V)$ est, d'après les Équations VI.3.10 et VI.3.11 :

$$f_S(s) = f_{(1-U)\cdot(1-V)}(s) = \int_0^1 f_U(1 - u) \cdot f_V(1 - (s / u)) \cdot (1 / u) \cdot du \qquad \text{[VI.3.12]}$$

De plus, la densité de probabilité de la variable aléatoire $Z = 1 - (1 - U) \cdot (1 - V)$ est, d'après les Équations VI.3.11 et VI.3.12 :

$$f_Z(z) = f_{1-(1-U)\cdot(1-V)}(z) = \int_0^1 f_U(1 - u) \cdot f_V(1 - ((1 - z) / u)) \cdot (1 / u) \cdot du \qquad \text{[VI.3.13]}$$

Finalement, avec le changement de variable $u' = 1 - u$:

$$f_Z(z) = f_{1-(1-U)\cdot(1-V)}(z) = \int_0^1 f_U(u') \cdot f_V(1 - ((u' - z) / (u' - 1))) \cdot (1 / (1 - u')) \cdot du \qquad \text{[VI.3.14]}$$

VI.2.4. Preuves des Équations III.3.10 et II.3.11

D'après l'Équation III.3.7 :

$\{V[X \cdot Y] \leq V[X]\}$ si et seulement si $\{(E^2[X] / V[X]) \leq (1 / V[Y]) - (E^2[Y] / V[Y]) - 1\}$ [VI.3.15]

De même :

$\{V[X \cdot Y] \leq V[Y]\}$ si et seulement si $\{(E^2[Y] / V[Y]) \leq (1 / V[X]) - (E^2[X] / V[X]) - 1\}$ [VI.3.16]

D'après les Équations VI.3.15 et VI.3.16 :

$\{V[X \cdot Y] \leq min(V[X], V[Y])\}$ si et seulement si

$\{(E^2[X] / V[X]) + (E^2[Y] / V[Y]) \leq (1 / max(V[X], V[Y])) - 1\}$ [VI.3.17]

La même approche est utilisée pour démontrer l'Équation II.3.11.

CHAPITRE VII

RÉFÉRENCES

La première section de ce chapitre présente les références bibliographiques citées dans ce mémoire de thèse, ordonnées par ordre alphabétique selon la première lettre du prénom du premier auteur, suivi des deux premières lettres du nom, et des deux derniers chiffres de l'année de publication. La seconde section présente les publications réalisées lors des travaux de thèse.

SOMMAIRE DU CHAPITRE VII

VII.1. RÉFÉRENCES CITÉES DANS CE MÉMOIRE DE THÈSE

[AAl10] A.W. Al-Dabbagh, L. Lu, "Reliability modeling of networked control systems using dynamic flowgraph methodology," *Reliability Engineering & System Safety*, vol. 95(11), p. 1202-1209, 2010.

[AAm84] A. Amendola, G. Reina, *DYLAM-1: A Software Package for Event Sequence and Consequence Spectrum Methodology, EUR 9224 EN*, Luxembourg: Commission of European Communities, 1984.

[ABo01] A. Bondavalli, M. Dal Cin, D. Latella, I. Majzik, A. Pataricza, G. Savoia, "Dependability analysis in the early phases of UML-based system design," *Computer and System Sciences Engineering*, vol. 16(5), p. 265-275, 2001.

[AGi96] A. Giua, E. Usai, "High-level hybrid petri nets: A definition," In: IEEE (ed), vol. 1-4, p. 148-150, New York: IEEE, 1996, *Proceedings of the 35th IEEE Conference on Decision and Control*, Kobe, Japan, December 11-13, 1996.

[AHa08] A. Hakobyan, T. Aldemir, R. Denning, S. Dunagan, D. Kunsman, B. Rutt, U. Catalyurek, "Dynamic generation of accident progression event trees," *Nuclear Engineering and Design*, vol. 238(12), p. 3457-346, 2008.

[AJa98] A. Jalashgar, "Identification of hidden failures in process control systems based on the HMG method," *International Journal of Intelligent Systems*, vol. 12(1-3), p. 159-179, 1998.

[AKl10] A. Kleyner, V. Volovoi, "Application of Petri nets to reliability prediction of occupant safety systems with partial detection and repair," *Reliability Engineering & System Safety*, vol. 95(6), p. 606-613, 2010.

[ALa08] A. Lannoy, *Maîtrise des risques et sûreté de fonctionnement – repères historiques et méthodologiques*, Paris: Lavoisier, 2008.

[ALa96] A. Lannoy, *Analyse quantitative et utilité du retour d'expérience pour la maintenance et la sécurité*, Paris: Eyrolles, 1996.

[AMk08] A. Mkhida, J.M. Thiriet, J.F. Aubry, "Toward an intelligent distributed safety instrumented systems: dependability evaluation," In: M.J. Chung, P. Misra (eds), vol. 16, *Proceedings of the 17th IFAC World Congress*, Coex, South Korea, 2008.

[AMo01] A.W. Moran, P.G. O'Reilly, G.W. Irwin, "Probability estimation algorithms for self-validating sensors," *Control Engineering Practice*, vol. 9(4), p. 425-438, 2001.

[AOH04] A. O'Hagan, J.E. Oakley, "Probability is perfect, but we can't elicit it perfectly," *Reliability Engineering & System Safety*, vol. 85(1-3), p. 239-248, 2004.

[Ara09] Aralia WorkShop, *http://www.arboost.com/arlshop-page.htm*, 2009.

[ARa03] A.V. Ratzer, L. Wells, H.M. Lassen, M. Laursen, J.F. Qvortrup, M.S. Stissing, M. Christensen, K. Jensen, "CPN Tools for Editing, Simulating, and Analysing Coloured Petri Nets," In: W. Van der Aalst, E. Best (eds), vol. 2679, p. 450-462, Berlin: Springer-Verlag, 2003, *Proceedings of the 24th International Conference on the Application and Theory of Petri Nets*, Eindhoven, The Netherlands, June 23-27, 2003.

[ARu88] A.M. Rushdi, K.F. Kafrawy, "Uncertainty propagation in fault-tree analyses using an exact method of moments," *Microelectronics Reliability*, vol. 26(6), p. 945-965, 1988.

[ASu00a] A.E. Summers, "Viewpoint on ISA TR84.0.02 - simplified methods and fault tree analysis," *ISA Transactions*, vol. 39(2), p. 125-131, 2000.

[ASu00b] A. Summers, B. Zachary "Partial-stroke testing of safety block valves," *Control Engineering*, vol. 47(12), p. 87-89, 2000.

[ASu99] A.E. Summers, G. Raney, "Common cause and common sense, designing failure out of your safety instrumented systems (SIS)," *ISA Transactions*, vol. 38(3), p. 291-299, 1999.

[ATa95] A.H. Taner, J.E. Brignell, "Aspects of intelligent sensor reconfiguration," *Sensors and Actuators A: Physical*, vol. 47(1-3), p. 525-529, 1995.

[ATo09] A.C. Torres-Echeverria, S. Martorell, H.A. Thompson, "Modelling and optimization of proof testing policies for safety instrumented systems," *Reliability Engineering & System Safety*, vol. 94(4), p. 838-854, 2009.

[BCo05] B. Conrard, J.M. Thiriet, M. Robert, "Distributed system design based on dependability evaluation: a case study on a pilot thermal process," *Reliability Engineering & System Safety*, vol. 88(1), p. 109-119, 2005.

[BDe04] B. Debray, E. Piatyszek, F. Cauffet, H. Londiche, *ARAMIS DIC, Appendix 7, Frequencies data for the fault tree*, Verneuil-en-Halatte: INERIS, 2004.

[BLa07] B. Lanternier, *Retour d'expérience et fiabilité prévisionnelle*, Thèse de doctorat, Saint-Etienne: Université Jean Monnet, 2007.

[BLa06] B. Lanternier, D. Charpentier, P. Lyonnet, "Failure rate model for spring loaded relief valves," In: C.G. Soares, E. Zio (eds), vol. 1-3, p. 905-909, London: Taylor & Francis group, 2006, *Proceedings of the European Safety and Reliability Conference*, Estoril, Portugal, Sptember 18-22, 2006.

[BT95] BT, *Handbook for Reliability Data for Components used in Telecommunication systems*, London: British Telecommunications, 1995.

[BTo96] B. Tombuyses, T. Aldemir, "Dynamic PSA of process control systems via continuous cell-to-cell mapping," In: C. Cacciabue, I.A. Papazoglou (eds), p. 1541-6154, London: Springer, 1996, *Proceedings of the European Safety and Reliability Conference/3th International Conference on Probabilistic Safety Assessment and Management*, Crete, Greece, 1996.

[BZh01] B.W. Zhang, M.S. Branicky, S.M. Philips, "Stability of Networked Control Systems," *IEEE Control Systems Magazine*, vol. 21(1), p. 84-99, 2001.

[CAc93] C. Acosta, N. Siu, "Dynamic event trees in accident sequence analysis: application to steam generator tube rupture," *Reliability Engineering & System Safety*, vol. 41(2), p. 135-154, 1993.

[CBe04] C. Benqlilou, M. Graells, E. Musulin, L. Puigjaner, "Design and retrofit of reliable sensor networks," *Industrial Engineering Chemistry Research*, vol. 43(25), p. 8026-8036, 2004.

[CCo07] C. Corsi, "Smart Sensors," *Infrared Physics and Technology*, vol. 49(3), p. 192-197, 2007.

[CCo06a] C. Cocozza-Thivent, R. Eymard, S. Mercier, "A finite volume scheme for dynamic reliability models," *IMA Journal of Numerical Analysis*, vol. 26(3), p. 446-471, 2006.

[CCo06b] C. Cocozza-Thivent, R. Eymard, S. Mercier, M. Roussignol, "Characterization of the marginal distributions of Markov processes used in dynamic reliability," *Journal of Applied Mathematics and Stochastic Analysis*, vol. 2006, p. 1-18, 2006.

[CCP99] CCPS, *CCPS Guidelines for Chemical Process Quantitative Risk Analysis, 2nd edition*, New-York: Wiley-AIChE, Center for Chemical Process Safety, 1999.

[CdE09] *Code de l'Environnement, Livre V : Prévention des pollutions, des risques et des nuisances (Partie legislative), Chapitre II : « Installations soumises à autorisation, à enregistrement ou à déclaration», Section 1 : Installations soumises à autorisation, Article L. 512-1 du code de l'environnement*, Paris, 2009.

[CE96] CE, *Directive 96/82/CE du Conseil du 9 décembre 1996 concernant la maîtrise des dangers lies aux accidents majeurs impliquant des substances dangereuses*, Conseil de l'Union Européen, 1996.

[CEC89] CEC, *Comparative analysis of a hypothetical loss-of flow accident in an irradiated LMFBR core using different computer models for a common benchmark problem, EUR 11925 EN*, Luxembourg: Commission of European Communities, 1989.

[CGa02] C.J. Garrett, G.E. Apostolakis, "Automated hazard analysis of digital control systems," *Reliability Engineering & System Safety*, vol. 77(1), p. 1-17, 2002.

[CGa95] C.J. Garrett, S.B. Guarro, G.E. Apostolakis, "The dynamic flowgraph methodology for assessing the dependability of embedded software systems," *IEEE Transactions on Systems Man Cybernetics*, vol. 25(5), p. 824-840, 1995.

[CIA05] CIAME, M. Bayart, B. Conrard, A. Chovin, M. Robert, "Capteurs et actionneurs intelligents," *Techniques de l'ingénieur*, vol. S7520, 2005.

[CIA87] CIAME, *Livre Blanc, Les capteurs intelligents : Réflexion des utilisateurs*, Paris: AFCET, 1987.

[Cir10] *Circulaire du 10/05/10 récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risqué à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003*, Paris, 2010.

[Cir06] *Circulaire n° DPPR/SEI2/CB-06-0388 du 28/12/06 relative à la mise à disposition du guide d'élaboration et de lecture des études de dangers pour les établissements soumis à autorisation avec servitudes et des fichies d'application des texts réglementaires récents*, Paris, 2005.

[Cir05] *Circulaire n° DPPR/SEI2/MM-05-0316 du 07/10/05 relative aux Installations Classées - Diffusion de l'ârrété ministériel relative à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation*, Paris, 2005.

[CKe04] C. Kermisch, P.E. Labeau, E. Lardeux, J.L. Chabot, "Implementation of hybrid Petri nets – Lessons learned from their application to a SMR unit," In: C. Spitzer, U. Schmocker, V.N. Dang (eds), vol. 1-6, p. 681-686, London: Springer-Verlag, 2004, *Proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management and the European Safety and Reliability Conference*, Berlin, Germany, June 14-18, 2004.

[CNN03] CNN.com, "Star survey reaches 70 sextillion," *CNN.com/Science and Space*, Wednesday, July 23, 2003.

[CPN10] CPN Tools, *http://wiki.daimi.au.dk/cpntools/*, 2010.

[CSh49] C.E. Shannon, W. Weaver, *The Mathematical Theory of Communication*, Urbana and Chicago: University of Illinois Press, 1949.

[CSm92] C. Smidts, J. Devooght, "Probabilistic reactor dynamics–II: A Monte Carlo study of a fast reactor transient," *Nuclear Science and Engineering*, vol. 111(3), p. 241-256, 1992.

[DCo72] D.R. Cox, "Regression models and life tables," *Journal of the Royal Statistical Society*, vol. 34(B), p. 187-220, 1972.

[DGa93] D.P. Gallegos, E.J. Bonano, "Consideration of uncertainty in the performance assessment of radioactive waste disposal from an international regulatory perspective," *Reliability Engineering & System Safety*, vol. 42(2-3), p. 111-123, 1993.

[DHu05] D.G. Hutcheson, "Moore's Law: The History and Economics of an Observation that Changed the World," *The Electrochemical Society INTERFACE*, vol. 14(1), p. 17-21, 2005.

[DLu95] D. Luttenbacher, S. Roth, M. Robert, C. Humbert, "Intelligent sensor: object approach," *Control Engineering Practice*, vol. 3(6), p. 805-812, 1995.

[DMa95] D. Martinez, D. Estève, "Adaptive quantization and fault detection in smart sensors," *Sensors and Actuators A: Physical*, vol. 47(1-3), p. 530-533, 1995.

[DRo77] D. Ross, "Structure Analysis (SA): a language for communicating ideas," *IEEE Transactions on Software Engineering*, vol. 3(1), p. 16-34, 1977.

[DSi90] D. Singer, "A fuzzy set approach to fault tree and reliability analysis," *Fuzzy Sets Systems*, vol. 34(2), p. 145-155, 1990.

[DVe03] D. Vernez, D. Buchs, G. Pierrehumbert, "Perspectives in the use of coloured Petri nets for risk analysis and accident modelling," *Safety Science*, vol. 41(5), p. 445-463, 2003.

[DZh07] D. Zhu, A. Mosleh, C. Smidts, "A framework to integrate software behavior into dynamic probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 92(12), p. 1733-1755, 2007.

[ECa99] E. Castillo, J.M. Sarabia, C. Solares, P. Gomez, "Uncertainty analyses in fault trees and Bayesian networks using FORM SORM methods," *Reliability Engineering & System Safety*, vol. 65(1), p. 29-40, 1999.

[ECE05] ECES, *EN 50402, Electrical apparatus for the detection and measurement of combustible or toxic gases vapours or of oxygen – Requirements on the functional safety of fixed gas detection systems*, Geneva: European Committee for Electrotechnical Standardisation, 2005.

[EEl90] E.A. Elsayed, C.K. Chan, "Estimation of thin-oxide reliability using proportional hazards models," *IEEE Transactions on Reliability*, vol. 39(3), p. 329-335, 1990.

[EXE01] EXERA, *Rapport d'enquête S 3782 X 01, Les systèmes de conduite de processus à base d'instrumentation intelligents sur les réseaux locaux industriels*, Paris : International Instrument Users' Associations, 2001.

[EZi09] E. Zio, F. Di Maio, "Processing dynamic scenarios from a reliability analysis of a nuclear power plant digital instrumentation and control system," *Annals of Nuclear Energy*, vol. 36(9), p. 1386-1399, 2009.

[EZi96] E. Zio, G.E. Apostolakis, "Two methods for the structured assessment of model uncertainty by experts in performance assessments of radioactive waste repositories," *Reliability Engineering & System Safety*, vol. 54(2-3), p. 225-241, 1996.

[FBa02a] F.G. Badía, M.D. Berrade, C.A. Campos, "Optimal inspection and preventive maintenance of units with revealed and unrevealed failures," *Reliability Engineering & System Safety*, vol. 78(2), p. 157-163, 2002.

[FBa02b] F. Bause, P.S. Kritzinger, *Stochastic Petri Nets – An introduction to the theory, 2nd edition*, Berlin: Vieweg Verlag, 2002.

[FBe95] F. Beaudouin, J.M. Favennec, M. Piguet, "Intelligent transmitters for process control – What, how, when, how much? A user's point of view," *ISA Transactions*, vol. 34(2), p. 199-207, 1995.

[FBrIP] F. Brissaud, B. Lanternier, D. Charpentier, "Modelling failure rates according to time and influencing factors," *International Journal of Reliability and Safety*, (in press).

[FBrPr] F. Brissaud, *Réseaux de Micro-Capteurs Sans-Fil*, Projet de rapport d'étude N° DRA-08-95406-11361A, Verneuil-en-Halatte: Institut National de l'Environnement Industriel et des Risques, (in press).

[FGu06] F. Guenab, D. Theilliol, P. Weber, Y.M. Zhang, D. Sauter, "Fault tolerant control system design: a reconfiguration strategy based on reliability analysis under dynamic behaviour constraints," In: Z. Zhang (ed), vol. 6, *Proceedings of the 6th IFAC symposium SAFEPROCESS*, Beijing, China, 2006.

[FIn10] F. Innal, Y. Dutuit, A. Rauzy, J.P. Signoret, "New insight into the average probability of failure on demand and the probability of dangerous failure per hour of

safety instrumented systems," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 224(2), p. 75-86, 2010.

[FIn06] F. Innal, Y. Dutuit, A. Rauzy, J.P. Signoret, "An attempt to understand better and apply some recommendations of IEC 61508 standard," In: H. Langseth, G. Cojazzi (eds), p. 1-16, *Proceedings of the 30th ESReDA seminar*, Trondheim, Norway, June 7-8, 2006.

[FLi02] F.L. Lian, J. Moyne, D. Tilbury, "Network Design Consideration for Distributed Control Systems," *IEEE Transactions on Control Systems Technology*, vol. 10(2), p. 297-307, 2002.

[FWa08] F.Y. Wang, D. Liu, *Networked Control Systems – Theory and Applications*, London: Springer-Verlag, 2008.

[GAp90] G. Apostolakis, "The Concept of Probability in Safety Assessment of Technological Systems," *Science*, vol. 250(4986), p. 1359-1364, 1990.

[GAp88] G. Apostolakis, "The interpretation of probability in probability safety assessments," *Reliability Engineering & System Safety*, vol. 23(4), p. 247-252, 1988.

[GAp77] G. Apostolakis, Y.T. Lee, "Methods for estimation of confidence bounds for top-event unavailability of fault trees," *Nuclear Engineering Design*, vol. 41(3), p. 411-419, 1977.

[GCo96] G. Cojazzi, "The DYLAM approach for the dynamic reliability analysis of systems," *Reliability Engineering & System Safety*, vol. 52(3), p. 279-296, 1996.

[GLe06] G. Levitin, T. Zhang, M. Xie "State probability of a series-parallel repairable system with two-types of failure states," *International Journal of Systems Sciences*, vol. 37(14), p. 1011-1020, 2006.

[GMe94] G.C.M Meijer, "Concepts and focus point for intelligent sensor systems," *Sensors and Actuators A: Physical*, vol. 41(1-3), p. 183-191, 1994.

[GMi01] G. Mintchell, "Use sensors intelligently," *Control Engineering*, January, 2001.

[GPe10] G.A. Pérez Castañeda, J.F. Aubry, N. Brinzei, "Performance assessment of systems including conflict in the context of dynamic reliability," *International Journal of Adaptive and Innovative Systems*, vol. 1(3-4), p. 233-247, 2010.

[GRa09] G. Rasse, *Les plans de prevention des risques technologiques au prisme de la vulnérabilité : Le point de vue du juriste*, Thèse de doctorat, Paris: École Nationale Supérieure des Mines, 2009.

[GSm95] G. Smith, M. Bowen, "Considerations for the utilization of smart sensors," *Sensors and Actuators A: Physical*, vol. 47(1-3), p. 521-524, 1995.

[GSt09] G. Stefanou, "The stochastic finite element method: Past, present and future," *Computer Methods in Applied Mechanics and Engineering*, vol. 198(9-12), p. 1031-1051, 2009.

[GTi00] G.Y. Tian, Z.X. Zhao, R.W. Baines, "A Fieldbus-based intelligent sensor," *Mechatronics*, vol. 10(8), p. 835-849, 2000.

[HAR99] HART Communication Foundation, *HART Field communication protocol – Application guide HCF LIT 34*, Austin: HART Communication Foundation, 1999.

[HFa07] H. Fang, H. Ye, M. Zhong, "Fault diagnosis of networked control systems," *Annual Reviews in Control*, vol. 31(1), p. 55-68, 2007.

[HGu07] H. Guo, X. Yang, "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering & System Safety*, vol. 92(9), p. 1267-1273, 2007.

[HLa07] H. Langseth, L. Portinale, "Bayesian networks in reliability," *Reliability Engineering & System Safety*, vol. 92(1), p. 92-108, 2007.

[HMa00] H. Ø. Madsen, P. Christensen, K. Lauridsen, "Securing the operational reliability of an autonomous mini-submarine," *Reliability Engineering & System Safety*, vol. 68(1), p. 7-16, 2000.

[HPa97] H.S. Pan, W.Y. Yun, "Fault tree analyses with fuzzy gates," *Computers and Industrial Engineering*, vol. 33(3-4), p. 569-572, 1997.

[HPh96] H. Pham, H. Wang, "Imperfect maintenance," *European Journal of Operational Research*, vol. 94(3), p. 425-438, 1996.

[HPr98] H. Procaccia, P. Aufort, S. Arsenis, *The European Industry Reliability Data Bank (EIReDA), 3rd edition*, Iraklion: Crete University Press, 1998.

[HSc94] H. Schodel, "Utilization of fuzzy techniques in intelligent sensors," *Fuzzy Sets and Systems*, vol. 63(3), p. 271-292, 1994.

[HSi96] H.A. Simon, *The sciences of the artificial, 3rd edition*, Cambridge: MIT Press, 1996.

[HYa96] H. Yamasaki, "What are the intelligent sensors," *Handbook of Sensors and Actuators*, vol. 3, p. 1-17, 1996.

[HZh08] H. Zhang, F. Dufour, Y. Dutuit, K. Gonzalez, "Piecewise deterministic Markov processes and dynamic reliability," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222(4), p. 545-551, 2008.

[IAk02] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks," *IEEE Communication Magazine*, vol. 40(8), p. 104-112, 2002.

[IDe98] I. Demongodin, N.T. Koussoulas, "Differential Petri nets: Representing continuous systems in a discrete-event world," *IEEE Transactions on Automatic Control*, vol. 43(4), p. 573-579, 1998.

[IEE07] IEEE, *1451, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators*, New-York: Institute of Electrical and Electronics Engineers, 2007.

[IEC10] IEC, *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, 2nd edition*, Geneva: International Electrotechnical Commission, 2010.

[IEC09] IEC, *IEC 61907, Communication Network Dependability Engineering, 1st edition*, Geneva: International Electrotechnical Commission, 2009.

[IEC06] IEC, *IEC 60770-3, Transmitters for use in industrial-process control systems, Part 3: Methods for performance evaluation of intelligent transmitters, 1st edition*, Geneva: International Electrotechnical Commission, 2006.

[IEC05] IEC, *IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, 1st edition*, Geneva: International Electrotechnical Commission, 2005.

[IEC04] IEC, *IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, 1st edition*, Geneva: International Electrotechnical Commission, 2004.

[IEC02] IEC, *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, 1st edition*, Geneva: International Electrotechnical Commission, 2002.

[IEC99] IEC, *IEC 60770, Transmitters for use in industrial-process control systems, 1st edition*, Geneva: International Electrotechnical Commission, 1999.

[IEC96] IEC, *IEC 61709, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion, 1st edition*, Geneva: International Electrotechnical Commission, 1996.

[IEC90] IEC, *IEC 60050-191, International Electrotechnical Vocabulary – Chapter 191, 1st edition*, Geneva: International Electrotechnical Commission, 1990.

[IKi03] I.S. Kim, S.W. Cheon, M.C. Kim, "Nuclear equipment parts classification: a functional modeling approach," *Annals of Nuclear Engineering*, vol. 30(16), p. 1677-1690, 2003.

[INE10] INERIS, *http://www.ineris.fr*, 2010.

[INE09] INERIS, Rapport scientifique 2008-2009, Verneuil-en-Halatte: Institut National de l'Environnement Industriel et des Risques, 2009.

[IPa03] I.A. Papazoglou, O.N. Aneziris, "Master logic diagram: method for hazard and initiating event identification in process plants," *Journal of Hazardous Materials*, vol. 97(1-3), p. 11-30, 2003.

[ISA04] ISA, *ANSI/ISA-84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Research Triangle Park: International Society of Automation, 2004.

[ISA93] ISA, *ANSI/ISA-51.1-1979 - (R1993), Process Instrumentation Terminology*, Research Triangle Park: International Society of Automation, 1993.

[IVB04] I. Van Beurden, R. Amkreutz, "'Proven-in-use' criteria for safety instrumented systems," *Hydrocarbon processing*, vol. 81(11), p. 61-70, 2004.

[JBr96] J.E. Brignell, "The future of intelligent sensors: A problem of technology or ethics?," *Sensors and Actuators A: Physical*, vol. 56(1-2), p. 11-15, 1996.

[JBu09] J.V. Bukowski, I. Van Beurden, "Impact of proof test effectiveness on safety instrumented system performance," In: IEEE (ed), p. 157-163, New York: IEEE, 2009, *Proceedings of the 55th Annual Reliability and Maintainability Symposium*, Ft Worth, USA, January 26-29, 2009.

[JBu08] J.V. Bukowski, "A Unified Model for Evaluating the Safety Integrity Level of Safety Instrumented Systems," In: IEEE (ed), p. 139-144, New York: IEEE, 2008, *Proceedings of the 54th Annual Reliability and Maintainability Symposium*, Las Vegas, USA, January 28-31, 2008.

[JBu06] J.V. Bukowski, "Using Markov models to compute probability of failed dangerous when repair times are not exponentially distributed," In: IEEE (ed), p. 273-277, New York: IEEE, 2006, *Proceedings of the 52nd Annual Reliability and Maintainability Symposium*, Newport Beach, USA, January 23-26, 2006.

[JBu05] J.V. Bukowski, "A comparison of techniques for computing PFD average," In: IEEE (ed), p. 590-595, New York: IEEE, 2005, *Proceedings of the 51st Annual Reliability and Maintainability Symposium*, Alexandria, USA, January 24-27, 2005.

[JBu01] J.V. Bukowski, "Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems," *IEEE Transactions on Reliability*, vol. 50(3), p. 321-329, 2001.

[JCa99] J.C. Campelo, P. Yuste, F. Rodriguez, P.J. Gil, J.J. Serrano, "Hierarchical reliability and safety models of fault tolerant distributed industrial control systems," In M. Felici, K. Kanoun, A. Pasquini (eds), vol. 1698, p. 202-215, Berlin: Springer-Verlag, 1999, *Proceedings of the 18th International Conference on Computer Safety, Reliability and Security*, Toulouse, France, September 27-29, 1999.

[JDe98] J. Devooght, "Uncertainty analysis in dynamic reliability," In: A. Mosleh, R.A. Bari (eds), vol. 1-4, p. 2263-2268, London: Springer-Verlag, 1998, *Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management*, New York, USA, September 13-18, 1998.

[JDe96] J. Devooght, C. Smidts, "Probabilistic dynamics as a tool for dynamic PSA," *Reliability Engineering & System Safety*, vol. 52(3), p. 185-196, 1996.

[JDe95] J. Devooght, P.E. Labeau, "Moments of the distributions in probabilistic dynamics," *Annals of Nuclear Energy*, vol. 22(2), p. 97-108, 1995.

[JDe92a] J. Devooght, C. Smidts, "Probabilistic reactor dynamics–III: A framework for time-dependent interaction between operator and reactor during a transient involving human error," *Nuclear Science and Engineering*, vol. 112(2), p. 101-113, 1992.

[JDe92b] J. Devooght, C. Smidts, "Probabilistic reactor dynamics–I: The theory of continuous event trees," *Nuclear Science and Engineering*, vol. 111(3), p. 229-250, 1992.

[JHe07] J.P. Hespanha, P. Naghshtabrizi, Y. Xu, "A Survey of Recent Results in Networked Control Systems," *Proceedings of the IEEE*, vol. 95(1), p. 138-162, 2007.

[JHe06] J.C. Helton, J.D. Johnson, C.J. Sallaberry, C.B. Storlie, "Survey of sampling-based methods for uncertainty and sensitivity analysis," *Reliability Engineering & System Safety*, vol. 91(10-11), p. 1175-1209, 2006.

[JHe04] J.C. Helton, J.D. Johnson, W.L. Oberkampf, "An exploration of alternative approaches to the representation of uncertainty in model predictions," *Reliability Engineering & System Safety*, vol. 85(1-3), p. 39-71, 2004.

[JHe96] J.C. Helton, D.E. Burmaster, "Guest editorial: treatment of aleatory and espistemic uncertainty in performance assessments for complex systems," *Reliability Engineering & System Safety*, vol. 54(2-3), 91-94, 1996.

[JKi09] J. Kirschenbaum, P. Bucci, M. Stovsky, D. Mandelli, T. Aldemir, M. Yau, S. Guarro, E. Ekici, S.A. Arndt, "A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems," *Nuclear Technology*, vol. 165(1), p. 53-95, 2009.

[JKi03] J.W. Kim, W. Jung, "A taxonomy of performance influencing factors for human reliability analysis of emergency tasks," *Journal of Loss Prevention in the Process Industries*, vol. 16(6), p. 479-495, 2003.

[JKn02] J.K. Knudsen, C.L. Smith, "Estimation of system failure probability uncertainty including model success criteria," In E.J. Bonano, A.L. Camp, M.J. Majors, R.A. Thompson (eds), p. 201-206, Kidlington: Elsevier Science Ltd, 2002, *Proceedings of the 6th International Probabilistic Safety Assessment and Management Conference*, San Juan, USA, June 23-28, 2002.

[JMe85] J.F. Meyer, A. Movaghar, W.H. Sanders, "Stochastic activity networks: structure, behaviour and application," In: IEEE (ed), p. 106-115, New York: IEEE, 1985, *Proceedings of the International Conference on Timed Petri Nets*, Torino, Italy, July 1-3, 1985.

[JO05a] JO n° 234 du 7 octobre 2005, *Arrêté du 29/09/05 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation, Titre II : Evaluation et prise en compte de la probabilité d'occurrence des phénomènes dangereux et accidents*, Paris, 2005.

[JO05b] JO n° 210 du 9 septembre 2005, *Décret n° 2005-1130 du 07/09/05 relatif aux plans de prévention des risques technologiques*, Paris, 2005.

[JO03] JO n° 175 du 31 juillet 2003, *Loi n°2003-699 du 30/07/03 relative à la prevention des risques technologiques et naturels et à la reparation des dommages, Chapitre II : Maîtrise de l'urbanisation autour des établissements industriels à risques, Article 4 de la loi du 30 juillet 2003*, Paris, 2003.

[JO76] JO du 20 juillet 1976, *Loi n° 76-663 du 19/07/76 relative aux ICPE*, Paris, 1976.

[JPe03] J. Pérez, M.S. Reorda, M. Violante, "Dependability analysis of CAN networks: an emulation-based approach," In: C. Bolchini, F. Lombardi, F.J. Meyer, R. Velazco, X. Sun (eds), p. 537-544, Los Amiltos: IEEE Computer Society, 2003, *Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, Boston, USA, November 3-5, 2003.

[JPe81] J.L. Peterson, *Petri Net Theory and the Modeling of Systems*, New York: Prentice-Hall, 1981.

[JPi02] J.R. Pimentel, M. Salazar, "Dependability of Distributed Control System Fault Tolerant Units," In: IEEE (ed), vol. 1-4, p. 3164-3169, New York: IEEE, 2002, *Proceedings of the 28th Annual Conference of the IEEE Industrial Electronics Society*, Seville, Spain, November 5-8, 2002.

[JRe06] J.M. Reinert, G.E. Apostolakis, "Including model uncertainty in risk-informed decision making," *Annals of Nuclear Energy*, vol. 33(4), p. 354-369, 2006.

[JRo06] J.L. Rouvroye, J.A. Wiegerinck, "Minimizing costs while meeting safety requirements: Modeling deterministic (imperfect) staggered tests using standard Markov models for SIL calculations," *ISA Transactions*, vol. 45(4), p. 611-621, 2006.

[JSi07a] J.P. Signoret, "High Integrity Protection Systems (HIPS) – Making SIL Calculations Effective," *Exploration and Production: The Oil and Gas Review*, p. 14-17, 2007.

[JSi07b] J.P. Signoret, Y. Dutuit, A. Rauzy, "High Integrity Protection Systems (HIPS): Methods and tools for efficient Safety Integrity Levels (SIL) analysis and calculations," In: T. Aven, J. Vinnem (eds), vol. 1-3, p. 663-669, London: Taylor & Francis group, 2007, *Proceedings of the European Safety and Reliability Conference*, Stavenger, Norway, June 25-27, 2007.

[JTh04] J.M. Thiriet, *Sûreté de fonctionnement de systèmes d'automatisation à intelligence distribuée*, Habilitation à diriger des recherches, Nancy: Université Henri Poincaré, 2004.

[JVa11] J.K. Vaurio, "Unavailability equations for k-out-of-n systems," *Reliability Engineering & System Safety*, vol. 96(2), p. 350-352, 2011.

[JYi08] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52(12), p. 2292-2330, 2008.

[KDa94] K. Davoudian, J.S. Wu, G. Apostolakis, "Incorporating organisational-factors into risk assessment through the analysis of work processes," *Reliability Engineering & System Safety*, vol. 45(1-2), p. 85-125, 1994.

[KHs96] K.S. Hsueh, A. Mosleh, "The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants," *Reliability Engineering & System Safety*, vol. 52(3), p. 297-314, 1996.

[KJe07] K. Jensen, L.M. Kristensen, L. Wells, "Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems," *International Journal on Software Tools for Technology Transfer*, vol. 9(3), p. 213-254, 2007.

[KJe02] K. Jensen, *Coloured Petri Nets: basic concepts, analysis methods and practical use, 2nd edition*, London: Springer-Verlag, 2002.

[KMi90] K.B. Misra, G.G. Weber, "Use of fuzzy set theory for level-I studies in probabilistic risk assessment," *Fuzzy Sets Systems*, vol. 37(2), p. 139-160, 1990.

[KTi95] K. Tindell, A. Burns, A.J. Wellings, "Calculating controller area network (CAN) message response times," *Control Engineering Practice*, vol. 3(8), p. 1163-1169, 1995.

[KØi01a] K. Øien, "A framework for the establishment of organizational risk indicators," *Reliability Engineering & System Safety*, vol. 74(2), p. 147-167, 2001.

[KØi01b] K. Øien, "Risk indicators as a tool for risk control," *Reliability Engineering & System Safety*, vol. 74(2), p. 129-145, 2001.

[LCa04] L. Cauffriez, J. Ciccotelli, B. Conrard, M. Bayart, "Design of intelligent distributed control systems: a dependability point of view," *Reliability Engineering & System Safety*, vol. 84(1), p. 19-32, 2004.

[LCa03] L. Cauffriez, B. Conrard, J.M. Thiriet, M. Bayart, "Fieldbuses and their influence on dependability," In: IEEE (ed), p. 83-88, New York: IEEE, 2003, *Proceedings of the IEEE Instrumentation & Measurement Technology Conference*, Vail, USA, May 20-22, 2003.

[LOl10] L.F. Oliveira, R.N.L Abramovitch, "Extension of ISA TR84.00.02 PFD equations to KooN architectures," *Reliability Engineering & System Safety*, vol. 95(7), p. 707-715, 2010.

[MBh08] M. Bhushan, S. Narasimhan, R. Rengaswamy, "Robust sensor network design for fault diagnosis," *Computer & Chemical Engineering*, vol. 32(4-5), p. 1067-1084, 2008.

[MBh00] M. Bhushan, R. Rengaswamy, "Robust sensor network design for fault diagnosis," *Computer & Chemical Engineering*, vol. 24(2-7), p. 735-741, 2000.

[MBl97] M. Blanke, R. Izadi-Zamanabadi, S.A. Bøgh, C.P. Lunau, "Fault-tolerant control systems - A holistic view," *Control Engineering Practice*, vol. 5(5), p. 693-702, 1997.

[MBo06] M. Boiteau, Y. Dutuit, A. Rauzy, J.P. Signoret, "The AltaRica data-flow language in use: modelling of production availability of a multi-state systems," *Reliability Engineering & System Safety*, vol. 91(7), p. 747-755, 2006.

[MBo03] M. Bouissou, J.L. Bon, "A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes," *Reliability Engineering & System Safety*, vol. 82(2), p. 149-163, 2003.

[MBr00] M.S. Branicky, S.M. Philips, W. Zhang, "Stability of Networked Control Systems: Explicit Analysis of Delay," In: AACC (ed), vol. 1-6, p. 2352-2357, New York: IEEE, 2000, *Proceedings of the American Control Conference*, Chicago, USA, June 28-30, 2000.

[MBr83] M. Brown, F. Porschan, "Imperfect repair," *Journal of Applied Probability*, vol. 20(4), p. 851-859, 1983.

[MCe02] M. Cepin, B. Mavko, "A dynamic fault tree," *Reliability Engineering & System Safety*, vol. 75(1), p. 83-91, 2002.

[MDa93] M.H.A. Davis, *Markov models and optimization, Monographs on statistics and applied probability series 49*, London: Chapman and Hall, 1993.

[MDa84] M.H.A. Davis, "Piecewise-deterministic Markov processes – a general class of non-diffusion stochastic models," *Journal of the Royal Statistical Society*, vol. 46(3), p. 353-388, 1984.

[MED07] MEDAD, *Le plan de prévention des risques technologiques (PPRT) – Guide méthodologique*, Paris: Ministère de l'Écologie, du Développement et de l'Aménagement Durable, 2007.

[MEE10a] MEEDM, *Dossier de presse – Chantal Jouanno présente les objectifs 2010 et le bilan 2009 de l'Inspection des installations classées*, Paris: Ministère de l'Écologie, de l'Energie, du Développement durable et de la Mer, 2010.

[MEE10b] MEEDM, *Communiqué de presse – Inspection des installations classées : Chantal Jouanno, secrétaire d'Etat à l'Ecologie présente le bilan et les priorités 2010 de l'inspection*, Paris: Ministère de l'Écologie, de l'Energie, du Développement durable et de la Mer, 2010.

[MEv97] M.H.C. Everdij, H.A.P. Blom, M.B. Klompstra, "Dynamically coloured petri nets for air traffic management safety purposes," In: M. Papageorgiou, A. Pouliezos (eds), vol. 1-3, p. 169-174, Oxford: Pergamon Press, 1997, *Proceedings of the 8th IFAC Symposium on Transportation Systems*, Chania, Greece, June 16-18, 1997.

[MGo99] M.W. Goble, "Safety Rated Smart Transmitters - Failure Modes and Diagnostic Analysis," *Proceedings of ISA TECH 1999*, Dusseldorf, Germany, 1999.

[MKl06] M. Kloos, J. Peschke, "MCDET: A probabilistic dynamics method combining Monte Carlo simulation with the discrete dynamic event tree approach," *Nuclear Science and Engineering*, vol. 153(2), p. 137-156, 2006.

[MKu08] M. Kumar, A. Verma, A. Srividya, "Modeling demand rate and imperfect proof-test and analysis of their effect on system safety," *Reliability Engineering & System Safety*, vol. 93(11), p. 1720-1729, 2008.

[MLa99] M. Lambert, B. Riera, G. Martel, "Application of functional analysis techniques to supervisory systems," *Reliability Engineering & System Safety*, vol. 64(2), p. 209-224, 1999.

[MLi94] M. Lind, "Modeling goals and functions of complex industrial-plants," *Applied Artificial Intelligence*, vol. 8(2), p. 259-283, 1994.

[MLu09] M.A. Lundteigen, M. Rausand, "Architectural constraints in IEC 61508: Do they have the intended effect?," *Reliability Engineering & System Safety*, vol. 94(2), p. 520-525, 2009.

[MLu08a] M.A. Lundteigen, M. Rausand, "Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas," *Reliability Engineering & System Safety*, vol. 93(8), p. 1208-1217, 2008.

[MLu08b] M.A. Lundteigen, M. Rausand, "Partial stroke testing of process shutdown valves: How to determine the test coverage," *Journal of Loss Prevention in the Process Industries*, vol. 21(6), p. 579-588, 2008.

[MLu07] M.A. Lundteigen, M. Rausand, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," *Journal of Loss Prevention in the Process Industries*, vol. 20(3), p. 218-229, 2007.

[MMa96] M. Marseguerra, E. Zio, "Monte Carlo approach to PSA for dynamic process systems," *Reliability Engineering & System Safety*, vol. 52(3), p. 227-241, 1996.

[MMe04] M.J.P. Meulen, "On the use of smart sensors, common cause failure and the need for diversity," In: TUV (ed), *Proceedings of the 6th International symposium programmable electronic systems in safety related applications*, Cologne, Germany, 2004.

[MMo99] M. Modarres, S.W. Cheon, "Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives," *Reliability Engineering & System Safety*, vol. 64(2), p. 181-200, 1999.

[MMo93] M. Modarres, "Functional modeling of complex systems using a GTST-MPLD framework," *Proceedings of the 1st International workshop on functional modeling of complex technical systems*, Ispra, Italy, 1993.

[MMo85a] M. Modarres, M.L. Roush, R.N. Hunt, "Application of goal trees in reliability allocations for systems and components of nuclear power plants," *Proceedings of the 12th INTER-RAM conference*, Baltimore, USA, 1985.

[MMo85b] M. Modarres, M.L. Roush, R.N. Hunt, "Application of goal trees for nuclear power plant hardware protection," *Proceedings of the 8th International conference on structural mechanics in reactor technology*, Brussels, Belgium, 1985.

[MNe94] M. Newby, "Perspective on Weibull Proportional-Hazards Models," *IEEE Transactions on Reliability*, vol. 43(2), p. 217-223, 1994.

[MRa02] M. Rausand, A. Høyland, *System reliability theory; models, statistical methods, and applications, 2nd edition*, New York: Wiley, 2002.

[MRa96] M. Rausand, K. Øien, "The basic concepts of failure analysis," *Reliability Engineering & System Safety*, vol. 53(1), p. 73-83, 1996.

[MRo93] M. Robert, M. Marchandiaux, M. Porte, *Capteurs intelligents et méthodologie d'évaluation*, Paris: Hermes, 1993.

[MRo85] M.L. Roush, M. Modarres, R.N. Hunt, "Application of goal trees to evaluation of the impact of information upon plant availability," *Proceedings of the ANS/ENS topical meeting on probabilistic safety methods and applications*, San Francisco, USA, 1985.

[MSc10] M. Schönbeck, M. Rausand, J. Rouvroye, "Human and organisational factors in the operational phase of safety instrumented systems: A new approach," *Safety Science*, vol. 48(3), p. 310-318, 2010.

[MSt05] M. Staroswiecki, "Intelligent sensors: A functional view," *IEEE Transactions on Industrial Informatics*, vol. 1(4), p. 238-249, 2005.

[MSt02] M. Stamatelatos, G. Apostolakis, H. Dezfuli, C. Everline, S. Guarro, P. Moieni, A. Mosleh, T. Paulos, R. Youngblood, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Version 1.1*, Washington DC: Office of Safety and Mission Assurance, NASA Headquarters, 2002.

[MYa98] M. Yau, G. Apostolakis, S. Guarro, "The use of prime implicants in dependability analysis of software controlled systems," *Reliability Engineering & System Safety*, vol. 62(1-2), p. 23-32, 1998.

[NBr09] N. Brinzei, G.A. Pérez Castañeda, J.F. Aubry, "Sûreté de fonctionnement prévisionnelle en contexte dynamique," *Proceedings of the 2ème Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes*, Nancy, France, June 3-4, 2009.

[NDu09] N. Duflot, C. Bérenguer, L. Dieulle, D. Vasseur, "A min cut-set-wise truncation procedure for importance measures computation in probabilistic safety assessment," *Reliability Engineering & System Safety*, vol. 94(11), p. 1827-1837, 2009.

[NEl05] N.H. El-Farra, A. Gani, P.D. Christofides, "Fault-Tolerant Control of Process Systems Using Communication Networks," *AIChE Journal*, vol. 51(6), p. 1665-1682, 2005.

[NNa00] N. Navet, Y.Q. Song, F. Simonot, "Worst-case deadline failure probability in real-time applications distributed over controller area network," *Journal of Systems architecture*, vol. 46(7), p. 607-617, 2000.

[NSi94] N. Siu, "Risk assessment for dynamic systems: An overview," *Reliability Engineering & System Safety*, vol. 43(1), p. 43-73, 1994.

[NSW98] NSWC, *NSWC-98/LE1, Handbook of Reliability Prediction Procedures for Mechanical Equipment*. Washington: Naval Surface Warfare Center, 1998.

[NWa01] N. Wattanapongsakorn, S. Levitan, "Reliability Optimization Models for Fault-Tolerant Distributed Systems," In: IEEE (ed), p. 193-199, New York: IEEE, 2001, *Proceedings of the Annual Reliability and Maintainability Symposium*, Philadelphia, USA, January 22-25, 2001.

[OMG07a] OMG, *OMG systems modeling language – OMG SysML, Version 1.0*, Needham: Object management group, 2007.

[OMG07b] OMG, *Unified modeling language, Version 2.0*, Needham: Object management group, 2007.

[OMG03] OMG, *Smart transducers interface specification*, Needham: Object management group, 2003.

[ORE09] OREDA Participants, *Offshore Reliability Data Handbook (OREDA 2009), 5th edition*, Trondheim: SINTEF Technology and Society, 2009.

[PBa03] P. Barger, J.M. Thiriet, M. Robert, "Safety analysis and reliability estimation of a networked control system," *Proceedings of the 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, USA, June 9-11, 2003.

[PBa02] P. Barger, J.M. Thiriet, M. Robert, "Dynamic reliability and availability evaluation and validation of distributed systems," In: IEEE (ed), vol. 1-2, p. 837-842, New

York: IEEE, 2002, *Proceedings of the 19th IEEE IMTC*, Anchorage, USA, May 21-23, 2002.

[PBi05] P. Bishop, R. Bloomfield, S. Guerra, K. Tourlas, "Justification of smart sensors for nuclear applications," In: R. Winther, B.A. Gran, G. Dahll (eds), vol. 3688, p. 194-207, Berlin: Springer-Verlag, 2005, *Proceedings of the 24th SAFECOMP*, Fredrikstad, Norway, 2005.

[PCa86] P.C. Cacciabue, A. Amendola, G. Cojazzi, "Dynamic logical analytical methodology versus fault tree: the case study of the auxiliary feedwater system of a nuclear power plant," *Nuclear Technology*, vol. 74(2), p. 195-208, 1986.

[PCo85] P. Courtois, "On Time and Space decomposition of complex structures," *Communications of the ACM*, vol. 28(6), p. 590-603, 1985.

[PDa10] P. David, V. Idasiak, F. Kratz, "Reliability study of complex systems using SysML," *Reliability Engineering & System Safety*, vol. 95(4), p. 431-450, 2010.

[PDa09] P. David, V. Idasiak, F. Kratz, "Towards a better interaction between design and dependability analysis: FMEA derived from UML/SysML models," In: S. Martorell, C.G. Soares, J. Barnett (eds), vol. 1-4, p. 2259-2266, Boca Raton: CRC Press, Taylor & Francis group, 2009, *Proceedings of the European Safety and Reliability Conference and the 17th Annual meeting of the SRA-Europe*, Valencia, Spain, September 22-25, 2009.

[Pet10] Petri Nets World, *http://www.informatik.uni-hamburg.de/TGI/PetriNets/*, 2010.

[PHo04] P. Hokstad, K. Corneliussen, "Loss of safety assessment and the IEC 61508 standard," *Reliability Engineering & System Safety*, vol. 83(1), p. 111-120, 2004.

[PHo95] P. Hokstad, P. Flotten, S. Holmstrom, F. McKenna, T. Onshus, "A reliability model for optimization of test schemes for fire and gas detectors," *Reliability Engineering & System Safety*, vol. 47(1), p. 15-25, 1995.

[Pic83] Pickard, Lowe and Garrick Inc, *Seabrook Station Probabilistic Safety Assessment, PLG-0300*, Newport Beach: (prepared for) Public Service Company of New Hampshire and Yankee Atomic Electric Company, 1983.

[PLa00] P.E. Labeau, C. Smidts, S. Swaminathan, "Dynamic reliability: towards an integrated platform for probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 68(3), p. 219-254, 2000.

[PLa97a] P.E. Labeau, Z.O. Amar, "Monte Carlo estimation of generalized unreliability in probabilistic dynamics .2. Handling uncertainties in parameters," *Nuclear Science and Engineering*, vol. 126(2), p. 146-157, 1997.

[PLa97b] P.E. Labeau, "Monte Carlo estimation of generalized unreliability in probabilistic dynamics .1. Application to a pressurized water reactor pressurizer," *Nuclear Science and Engineering*, vol. 126(2), p. 131-145, 1997.

[PLa96] P.E. Labeau, "A Monte Carlo estimation of the marginal distributions in a problem of probabilistic dynamics," *Reliability Engineering & System Safety*, vol. 52(1), p. 65-75, 1996.

[PNe07] P. Nelson, S.W. Wang, "Dynamic reliability via computational solution of generalized state-transition equations for entry-time processes," *Reliability Engineering & System Safety*, vol. 92(9), p. 1281-1293, 2007.

[PPo04] P. Portugal, A. Carvalho, "A framework for dependability evaluation of fieldbus networks," In: T. Sauter, F. Vasques (eds), p. 389-392, New York: IEEE, 2004, *Proceedings of the 5th International Workshop on Factory Communication Systems*, Vienna, Austria, September 22-24, 2004.

[PSk08] P. Sknourilova, R. Bris, "Coloured Petri nets and a dynamic reliability problem," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222(4), p. 635-642, 2008.

[PTr08] P. Trucco, E. Cagno, F. Ruggeri, O. Grande, "A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation," *Reliability Engineering & System Safety*, vol. 93(6), p. 823-834, 2008.

[RBa75] R.E Barlow, F. Proschan, *Statistical Theory of Reliability and Life Testing; Probability Models*, New York: Holt, Rinehart and Winston, 1975.

[RDa10] R. David, H. Alla, *Discrete, Continuous, and Hybrid Petri Nets, 2nd edition*, Berlin: Springer, 2010.

[RDa94] R. David, H. Alla, "Petri nets for modeling of dynamic systems: A survey," *Automatica*, vol. 30(2): 175-202, 1994.

[REy08] R. Eymard, S. Mercier, "Comparison of numerical methods for the assessment of production availability of a hybrid system," *Reliability Engineering & System Safety*, vol. 93(1), p. 168-177, 2008.

[RGh11] R. Ghostine, J.M. Thiriet, J.F. Aubry, "Variable delays and message losses: Influence on the reliability of a control loop," *Reliability Engineering & System Safety*, vol. 96(1), p. 160-171, 2011.

[RGh06] R. Ghostine, J.M. Thiriet, J.F. Aubry, "Dependability evaluation of networked control systems under transmission faults," In: Z. Zhang (ed), vol. 6, 2006, *Proceedings of the 6th IFAC symposium SAFEPROCESS*, Beijing, China, 2006.

[RGu08] R.A. Gupta, M.Y. Chow, "Overview of Networked Control Systems," Book chapter in *Networked Control Systems – Theory and Applications*, London: Springer-Verlag, 2008.

[RHu84] R.N. Hunt, M. Modarres, "Integrated economic risk management in a nuclear power plant," *Proceedings of the Annual meeting of the society for risk analysis*, Knoxville, USA, 1984.

[RIA06] RIAC, *Handbook of 217PlusTM Reliability Prediction Models*, Ultica: Reliability Information Analysis Center, 2006.

[RIA97] RIAC, *Electronic Parts Reliability Data (EPRD-97)*, Ultica: Reliability Information Analysis Center, 1997.

[RIA95] RIAC, *Nonelectronic Parts Reliability Data (NPRD-95)*, Ultica: Reliability Information Analysis Center, 1995.

[RRo98] R. Rosness, "Risk Influence Analysis, A methodology for identification and assessment of risk reduction strategies," *Reliability Engineering & System Safety*, vol. 60(2), p. 153-165, 1998.

[RWi96] R.L. Winkler, "Uncertainty in probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 54(2-3), p. 127-132, 1996.

[SDi06] S. Distefano, A. Puliafito, "Dynamic reliability block diagrams VS dynamic fault trees," In: IEEE (ed), p. 71-76, New York: IEEE, 2006, *Proceedings of the 53rd Annual Reliability and Maintainability Symposium*, Orlando, USA, January 22-25, 2007.

[SIN10] SINTEF Technology and Society, *Reliability Data for Safety Instrumented Systems – PDS Data Handbook, 2010 edition*, Trondheim: SINTEF Technology and Society, 2010.

[SKa91] S. Kaplan, *Risk Assessment and Risk Management – Basic Concepts and Terminology*, Boston: Hemisphere Publishing Corporation, 1991.

[SRo96] S.M. Ross, *Stochastic processes, 2nd edition*, USA: John Wiley & Sons, 1996.

[SSh08] S.K. Shin, P.H. Seong, "Review of various dynamic modeling methods and development of an intuitive modeling method for dynamic systems," *Nuclear Engineering and Technology*, vol. 40(5), p. 375-386, 2008.

[SSw00] S. Swaminathan, C. Smidts, "An application of the ESD framework to the probabilistic risk assessment of dynamic systems," In: S. Kondo, K. Furuta (eds),

vol. 1-4, p. 1283-1289, Tokyo: Universal Academy Press, 2000, *Proceedings of the 5th International Conference on Probabilistic Safety Assessment and Management*, Osaka, Japan, November 27-December 1, 2000.

[SSw99] S. Swaminathan, C. Smidts, "The event sequence diagram framework for dynamic probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 63(1), p. 73-90, 1999.

[TAl10] T. Aldemir, S. Guarro, D. Mandelli, J. Kirschenbaum, L.A. Mangan, P. Bucci, M. Yau, E. Ekici, D.W. Miller, X. Sun, S.A. Arndt, "Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies," *Reliability Engineering & System Safety*, vol. 95(10), p. 1011-1039, 2010.

[TAl06] T. Aldemir, D.W. Miller, M.P. Stovsky, J. Kirschenbaum, P. Bucci, A.W. Fentiman, L.A. Mangan, *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901*, Washington DC: U.S. Nuclear Regulatory Commission, 2006.

[TAl96] T. Aldemir, N. Siu, "Reliability and safety analysis of dynamic process systems – Guest editorial," *Reliability Engineering & System Safety*, vol. 52(3), p. 181-183, 1996.

[TAl94] T. Aldemir, N. Siu, P. Cacciabue, B. Göktepe, A. Molesh, *Reliability and Safety Assessment of Dynamic Process Systems, NATO ASI series, Series F: computer and system sciences*, Berlin: Springer, 1994.

[TAl91] T. Aldemir, "Utilization of the cell-to-cell mapping technique to construct Markov failure models for process control systems," In: G. Apostolakis (ed), vol. 2, p. 1431-1436, New York: Elsevier, 1991, *Proceedings of the 1th International Conference on Probabilistic Safety Assessment and Management*, Beverly Hills, USA, February 4-7, 1991.

[TAl87] T. Aldemir, "Computer-assisted Markov failure modeling of process control systems," *IEEE Transactions on Reliability*, vol. R-36(1), p. 133-144, 1987.

[TAv06] T. Aven, S. Sklet, J.E. Vinnem, "Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part 1. Method description," *Journal of hazardous Materials*, vol. 137(2), p. 681-691, 2006.

[Tel01] Telcordia Technology Inc., *Telcordia standard, Reliability Procedure for Electronic Equipment*, Piscataway: Telcordia Corporate, 2001.

[TMa96] T. Matsuoka, M. Kobayashi, "An analysis of a dynamic system by the GO-FLOW methodology," *Proceedings of the European Safety and Reliability Conference and the 3th International Conference on Probabilistic Safety Assessment and Management*, Crete, Greece, June 24-28, 1996.

[TMa88] T. Matsuoka, M. Kobayashi, "GO-FLOW: a new reliability analysis methodology," *Nuclear Science and Engineering*, vol. 98(1), p. 64-78, 1988.

[TMu89] T. Murata, "Petri Nets: Properties, Analysis and Applications," *Proceedings of the IEEE*, vol. 77(4), p. 541-580, 1989.

[TNa87] T. Nakagawa, K. Yasui, "Optimal policies for a system with imperfect maintenance," *IEEE Transactions on Reliability*, vol. 36(5), p. 631-633, 1987.

[TZh08] T.L. Zhang, Y.M. Wang, M. Xie, "Analysis of the Performance of Safety-Critical Systems with Diagnosis and Periodic Inspection," In: IEEE (ed), p. 145-150, New York: IEEE, 2008, *Proceedings of the 54th Annual Reliability and Maintainability Symposium*, Las Vegas, USA, January 28-31, 2008.

[TZh03] T. Zhang, W. Long, Y. Sato, "Availability of systems with self-diagnosis components–applying Markov model to IEC 61508-6," *Reliability Engineering & System Safety*, vol. 80(2), p. 133-141, 2003.

[UHa08] U. Hauptmanns, “The impact of reliability data on probabilistic safety calculation,” *Journal of Loss Prevention in the Process Industries*, vol. 21(1), p. 38-49, 2008.

[USD91] US DoD, *MIL-HDBK-127F, Reliability Prediction of Electronic Equipment*, Philadelphia: United States Department of Defence, 1991.

[USN02] US NRC, *Regulatory guide 1.174, An approach for using probabilities risk assessment in risk-informed decisions on plant-specific changes to the licensing basis, Revision 1*, Washington DC: US Nuclear Regulatory Commission, 2002.

[USN75] US NRC, *Reactor Safety Study (WASH-1400), NUREG-75/014*, Washington DC: U.S. Nuclear Regulatory Commission, 1975.

[UTE04] UTE, *Reliability Methodology for Electronic Systems – FIDES Guide 2004, issue A*, Fontenay-aux-Roses: Union Technique de l’Électricité, 2004.

[UTE03] UTE, *RDF 2003: Reliability Data Handbook*, Fontenay-aux-Roses: Union Technique de l’Électricité, 2003.

[VBe08] V. Benard, L. Cauffriez, D. Renaux, “The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems,” *Reliability Engineering & System Safety*, vol. 93(2), p. 179-196, 2008.

[VRo76] V.K. Rohatgi, *An introduction to probability theory and mathematical statistics*, New York: Wiley, 1976.

[VVo04] V. Volovoi, “Modeling of system reliability Petri nets with aging tokens,” *Reliability Engineering & System Safety*, vol. 84(2), p. 149-161, 2004.

[WLa10a] W.L. Lair, R. Ziani, S. Mercier, M. Roussignol, “Processus markoviens déterministes par morceaux et quantification déterministe avec un schéma de volumes finis : un cas d’étude,” In: IMdR (eds), 2010, *Proceedings of the 17ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, La Rochelle, France, October 5-7, 2010.

[WLa10b] W. Lair, R. Ziani, S. Mercier, M. Roussignol, “Modeling and quantification of aging systems for maintenance optimization,” In: IEEE (ed), New York: IEEE, 2010, *Proceedings of the 56th Annual Reliability and Maintainability Symposium*, San Jose, USA, January 25-29, 2010.

[WOb04] W.L. Oberkampf, J.C. Helton, C.A. Joslyn, S.F. Wojtkiewicz, S. Ferson, “Challenge problems: uncertainty in system response given uncertain parameters,” *Reliability Engineering & System Safety*, vol. 85(1-3), p. 11-19, 2004.

[YDa03] Y.S. Dai, M. Xie, K.L. Poh, G.Q. Liu, “A study of service reliability and availability for distributed systems,” *Reliability Engineering & System Safety*, vol. 79(1), p. 103-112, 2003.

[YDu08a] Y. Dutuit, A.B. Rauzy, J.P. Signoret, “A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems,” *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222(3), p. 371-379, 2008.

[YDu08b] Y. Dutuit, F. Innal, A.B. Rauzy, J.P. Signoret, “Probabilistic assessments in relationship with safety integrity levels by using Fault Trees,” *Reliability Engineering & System Safety*, vol. 93(12), p. 1867-1876, 2008.

[YDu97a] Y. Dutuit, A. Rauzy, “Exact and truncated computations of prime implicants of coherent and non-coherent fault trees within Aralia,” *Reliability Engineering & System Safety*, vol. 58(5), p. 127-144, 1997.

[YDu97b] Y. Dutuit, E. Chatelet, J.P. Signoret, P. Thomas, “Dependability modelling and evaluation by using stochastic Petri nets: Application to two test cases,” *Reliability Engineering & System Safety*, vol. 55(2), p. 117-124, 1997.

[YGe07] Y. Ge, L. Tian, Z. Liu, “Survey on the stability of networked control systems,” *Journal of Control Theory and Applications*, vol. 5(5), p. 374-379, 2007.

[YHu99] Y. Hu, M. Modarres, "Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modelling," *Reliability Engineering & System Safety*, vol. 64(2), p. 241-269, 1999.

[YHu96] Y.S. Hu, M. Modarres, "Time-dependent system knowledge representation based on dynamic master logic diagrams," *Control Engineering Practice*, vol. 4(1), p. 89-98, 1996.

[YLa08] Y. Langeron, A. Barros, A. Grall, C. Bérenguer, "Combination of safety integrity levels (SILs): A study of IEC61508 merging rules," *Journal of Loss Prevention in the Process Industries*, vol. 21(4), p. 437-449, 2008.

[YLa07] Y. Langeron, A. Barros, A. Grall, C. Bérenguer, "Safe failure impact on safety instrumented systems," In: T. Aven, J. Vinnem (eds), vol. 1, p. 641-648, London: Taylor & Francis group, 2007, *Proceedings of the European Safety and Reliability Conference*, Stavenger, Norway, June 25-27, 2007.

[YTi03] Y. Tipsuwan, M.Y. Chow, "Control methodologies in networked control systems," Control Engineering Practice, vol. 11(10), p. 1099-1111, 2003.

[YYa95] Y.Y. Yang, D.A. Linkens, S.P. Banks, "Modelling of hybrid systems based on extended coloured Petri nets," In: P. Antsaklis, W. Kohn, A. Nerode, S. Sastry (eds), vol. 999, p. 509-528, Berlin: Springer-Verlag, 1995, *Proceedings of the 3rd Workshop on Hybrid Systems II*, New York, USA, October 28-30, 1994.

[ZMa07] Z. Mao, B. Jiang, "Fault identification and fault-tolerant control for a class of networked control systems," *International Journal of Innovative Computing, Information and Control*, vol. 3(5), p. 1121-1130, 2007.

VII.2. PUBLICATIONS RÉALISÉES AU COURS DES TRAVAUX DE THÈSE

VII.2.1. Sûreté de Fonctionnement de Systèmes Instrumentés de Sécurité

[FBr10f] F. Brissaud, D. Charpentier, M. Fouladirad, A. Barros, C. Bérenguer, "Failure rate evaluation with influencing factors," *Journal of Loss Prevention in the Process Industries*, vol. 23(2), p. 187-193, 2010. doi: 10.1016/j.jlp.2009.07.013.

[FBr10g] F. Brissaud, A. Barros, C. Bérenguer, "Probability of Failure of Safety-Critical Systems Subject to Partial Tests," In: IEEE (ed), New York: IEEE, 2010, *Proceedings of the 56th Annual Reliability and Maintainability Symposium*, San Jose, USA, January 25-29, 2010.

[FBr09a] F. Brissaud, A. Barros, C. Bérenguer, "Politiques de Tests Partiels & Systèmes de Sécurité," *Proceedings of the 4ème édition du congrès international francophone Performances et Nouvelles Technologies en Maintenance*, Autrans, France, December 7-8, 2009.

[FBr09e] F. Brissaud, B. Lanternier, "Les Probabilités de Défaillance comme indicateurs de performance des Barrières Techniques de Sécurité – Approche analytique," *Proceedings of the 8ème congrès international pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement Durable*, Besançon, France, March 18-20, 2009.

[FBr08b] F. Brissaud, D. Charpentier, M. Fouladirad, A. Barros, C. Bérenguer, "Safety instrumented system reliability evaluation with influencing factors," In: S. Martorell, C.G. Soares, J. Barnett (eds), *Safety, Reliability and Risk Analysis: Theory and Applications*, vol. 1-4, p. 2003-2011, Boca Raton: CRC Press, Taylor & Francis group, 2009, *Proceedings of the European Safety and Reliability Conference and the 17th Annual Meeting of the Society for Risk Analysis Europe*, Valencia, Spain, September 22-25, 2008.

[FBr07] F. Brissaud, B. Lanternier, D. Charpentier, P. Lyonnet, "Modélisation des taux de défaillance en mécanique," *Proceedings of the 3ème édition du colloque international francophone Performances et Nouvelles Technologies en Maintenance*, Mons, Belgique, July 9-10, 2007.

VII.2.2. Modélisation et Évaluation de Capteurs-Transmetteurs à Fonctionnalités Numériques

[FBr11] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, "Reliability analysis for new technology-based transmitters," *Reliability Engineering & System Safety*, vol. 96(2), p. 299-313, 2011. doi: 10.1016/j.ress.2010.09.010.

[FBr10a] F. Brissaud, A. Barros, C. Bérenguer, "Handling Parameter and Model Uncertainties by Continuous Gates in Fault Tree Analyses," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, special issue on Uncertainty in Engineering Risk and Reliability, vol. 224(4), p. 253-265, 2010. doi: 10.1243/1748006XJRR313.

[FBr10c] F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, "Capteurs intelligents : Nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement," In: P. Kahn, A. Lannoy, D. Person-Silhol, D. Vasseur (eds), *Anticipation, innovation, perception : des défis pour la maîtrise des risques à l'horizon 2020*, Chapter 5, Paris: Lavoisier, 2010.

[FBr09b] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, "Design of complex safety-related systems in accordance with IEC 61508," In: R. Bris, C. Guedes Soares, S. Martorell (eds), *Reliability, risk and safety: theory and applications*, p. 1555-1562, Boca Raton: CRC Press, Taylor & Francis group, 2009, *Proceedings of the European Safety and Reliability Conference*, Prague, Czech Republic, September 7-10, 2009.

[FBr09c] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, "Reliability Study of an Intelligent Transmitter," In: H. Pham, T. Nakagawa (eds), *15th ISSAT International Conference on Reliability and Quality in Design*, p. 224-233, Piscataway: ISSAT, 2009, *Proceedings of the 15th ISSAT International Conference on Reliability and Quality in Design*, San Francisco, USA, August 6-8, 2009.

[FBr09d] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, "Dependability Issues for Intelligent Transmitters and Reliability Pattern Proposal," In: N. Bakhtadze, A. Dolgui (eds), *Information Control Problems in Manufacturing*, vol. 13, part 1, 2010, *Proceedings of the 13th IFAC Symposium on Information Control Problems in Manufacturing*, Moscow, Russia, June 3-5, 2009.

[FBr08a] F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, "Capteurs intelligents : Nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement," In: IMdR (eds), 2008, *Proceedings of the 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Avignon, France, October 6-10, 2008.

VII.2.3. Systèmes de Contrôle-Commande intégrant des Capteurs-Transmetteurs à Fonctionnalités Numériques

[FBrXX] F. Brissaud, C. Smidts, A. Barros, C. Bérenguer, "Dynamic Reliability of Digital-Based Transmitters," *Reliability Engineering & System Safety*, (in press). doi: 10.1016/j.ress.2010.12.014.

[FBr10b] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, "Fiabilité des Capteurs-Transmetteurs intégrant des Fonctionnalités Numériques," In: IMdR (eds), 2010, *Proceedings of the 17ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, La Rochelle, France, October 5-7, 2010.

[FBr10d] F. Brissaud, C. Smidts, A. Barros, C. Bérenguer, "Dynamic Reliability Modeling of Cooperating Digital-Based Systems," In: B.J.M. Ale, I.A. Papazoglou, E. Zio (eds), *Reliability, Risk and Safety: Back to the Future*, Boca Raton: CRC Press, Taylor & Francis Group, 2010, *Proceedings of the European Safety and Reliability Conference*, Rhodes, Greece, September 5-9, 2010.

[FBr10e] F. Brissaud, A. Barros, C. Bérenguer, "Improving availability and safety of control systems by cooperation between intelligent transmitters," *Proceedings of the 10th International Probabilistic Safety Assessment and Management Conference*, Seattle, USA, June 7-11, 2010.

RÉSUMÉS

Résumé en Français

L'utilisation de nouvelles technologies au sein des systèmes relatifs à la sécurité soulève des problèmes en termes de maîtrise des risques technologiques, et il est nécessaire de disposer d'outils d'évaluation probabiliste adaptés à la complexité accrue de ces systèmes. Les travaux présentés dans ce mémoire apportent des contributions à l'évaluation de la sûreté de fonctionnement des systèmes de sécurité, et en particulier des capteurs-transmetteurs à fonctionnalités numériques qui combinent l'acquisition de données avec des fonctions avancées de traitement et de transmission de l'information. L'objectif est d'étendre les méthodes de modélisation de la sûreté de fonctionnement, afin de mieux prendre en compte les diverses interactions et les comportements dynamiques mis en jeu par ces systèmes.

Le premier modèle proposé permet de représenter les aspects fonctionnels et matériels d'un système de sécurité, les défauts et défaillances, ainsi que les diverses relations entre éléments. Cette modélisation sert de support à des analyses de fiabilité et à des analyses d'incertitudes liées aux paramètres et au modèle. Une seconde contribution considère les capteurs-transmetteurs comme éléments de systèmes de contrôle-commande et vise à modéliser les interactions entre ces capteurs-transmetteurs, celles avec d'autres éléments du système, ainsi qu'avec le processus contrôlé, dans une approche de fiabilité dynamique.

Summary in English

The use of new technologies in safety-related systems gives rise to specific issues with respect to risk management, and it needs having probabilistic evaluation tools adapted to the increasing complexity of systems. The thesis works presented in this dissertation contribute to the dependability evaluation of safety-related systems, and especially for digital-based transmitters, which combine data acquisition with information processing and transmission. The aim is to extend the dependability modelling methods in order to take at best the various interactions and dynamic behaviours of the systems into account.

The first proposed model allows to represent the functional and material aspects of a safety system, the faults and failures, as well as the different relations between elements. This modelling framework is used as support to perform reliability analyses and uncertainty analyses with regard to parameters and model. A second contribution assumes the transmitters as part of control systems and aims to model the interactions between transmitters, and the interactions with the other systems' components and the process, using a dynamic reliability framework.